

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

OSCAR LEONARDO ALFONSO PRIETO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBIT
INGENIERIA ELECTRONICA
ZIPAQUIRA
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

OSCAR LEONARDO ALFONSO PRIETO

Diplomado de opción de grado presentado para optar el
Título de INGENIERO ELECTRONICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBIT
INGENIERIA ELECTRONICA
ZIPAQUIRA
2021

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

ZIPAQUIRA, 02 de diciembre de 2021

AGRADECIMIENTOS

En las presentes paginas se ve reflejada la guía he inspiración de Dios que inunda nuestro ser de fuerza para no desfallecer ante las dificultades académicas, en muchas ocasiones la desesperación por no tener el suficiente tiempo para cumplir con los requerimientos educativos el detenerse un momento y elevar una oración nos recarga de fuerzas para continuar y en todas las ocasiones nos muestra el camino a seguir.

Nuestras familias que en ocasiones pareciera que no estuvieran a nuestro lado apoyándonos, lo hacen al permitirnos los espacios de estudio viendo como nos aislamos y alejamos de ellos dejando de lado momentos en familia. A todos ellos muchas gracias.

A los Tutores de la universidad UNAD con los cuales tuve la oportunidad de interactuar, por el acompañamiento y por guiarnos en la construcción de conocimientos y sabiduría que al final se convertirán en una mejor calidad de vida para nosotros y nuestras familias.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO	5
LISTA DE TABLAS.....	7
LISTA DE FIGURAS	8
GLOSARIO	10
RESUMEN	11
ABSTRACT.....	12
INTRODUCCION	13
DESARROLLO	14
1. ESCENARIO 1	14
OBJETIVOS	15
ESCENARIO	15
Recursos necesarios	16
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces	16
Paso 1: Cablear la red como se muestra en la topología	16
Paso 2: Configurar los parámetros básicos para cada dispositivo	17
2 Parte 2: Configurar la capa 2 de la red y el soporte de Host	27
2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	29
2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.	32
2.3 En todos los switches habilite el protocoloRapid Spanning-Tree (RSTP)	35
2.4 En D1 y D2, configure los puentes raíz RSTP(root bridges) según la información del diagrama de topología.	37
2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	38
2.6 En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.....	41
2.7 Verifique los servicios DHCP IPv4.	44
2.8 Verifique la conectividad de la LAN local	45
3 Parte 3: Configurar los protocolos de enrutamiento	46

3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.....	48
3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.....	52
3.3	En R2 en la “Red ISP”, configure MP-BGP.....	56
3.4	En R1 en la “Red ISP”, configure MP-BGP.....	57
4	Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)	58
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	60
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	61
4.3	En D1, configure HSRPv2.....	62
5	Seguridad.	68
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de inscripción SCRYPT.	69
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de inscripción SCRYPT.	69
5.3	En todos los dispositivos (Excepto R2) habilite AAA	70
5.4	En todos los dispositivos (excepto R2) configure las especificaciones del servidor RADIUS.....	71
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA. 72	
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	72
6	Configure las funciones de Administración de Red.	72
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	72
6.2	Configure R2 como un NTP maestro.....	73
6.3	Configure NTP en R1, R3, D1, D2, y A1.	73
6.4	Configure Syslog en todos los dispositivos excepto en R2.	74
6.5	Configure SNMPv2c en todos los dispositivos excepto R2.	75
	CONCLUSIONES	77
	BIBLIOGRAFIA	78

LISTA DE TABLAS

Tabla 1 Tabla de direccionamiento15

Tabla 2 Configurar la capa 2 de la red y el soporte de Host28

Tabla 3 Configurar los protocolos de enrutamiento.....46

Tabla 4 Configurar la Redundancia del Primer Salto (First Hop Redundancy)58

LISTA DE FIGURAS

Ilustración 1 Topología de Red	14
Ilustración 2 Modelo distribución de red y conexaso17	17
Ilustración 3 Configuración inicial Router R1.....18	18
Ilustración 4 Configuración inicial Router R2.....19	19
Ilustración 5 Configuración inicial Router R3.....20	20
Ilustración 6 Configuración inicial Swich D122	22
Ilustración 7 Configuración inicial Swich D122	22
Ilustración 8 Configuración inicial Swich D224	24
Ilustración 9 Configuración inicial Swich D225	25
Ilustración 10 Configuración inicial Swich A126	26
Ilustración 11 Configuración inicial Swich A126	26
Ilustración 12 Configuración inicial PC127	27
Ilustración 13 configuración inicial PC2.....27	27
Ilustración 14 configuración interfaces troncales IEEE 802.1Q Swich D130	30
Ilustración 15 configuración interfaces troncales IEEE 802.1Q Swich D231	31
Ilustración 16 configuración interfaces troncales IEEE 802.1Q Swich A132	32
Ilustración 17 cambio la VLAN nativa en los enlaces troncales D133	33
Ilustración 18 cambio la VLAN nativa en los enlaces troncales D234	34
Ilustración 19 cambio la VLAN nativa en los enlaces troncales A135	35
Ilustración 20 configuración rapid-pvst en D1.....35	35
Ilustración 21 configuración rapid-pvst en D2.....36	36
Ilustración 22 configuración rapid-pvst en A1.....37	37
Ilustración 23 configuración puente Raíz D138	38
Ilustración 24 configuración puente Raíz D238	38
Ilustración 25 configuración EtherChannels LACP D1.....39	39
Ilustración 26 configuración EtherChannels LACP D2.....40	40
Ilustración 27 configuración EtherChannels LACP A141	41
Ilustración 28 configuración puertos de acceso del host D142	42
Ilustración 29 configuración puertos de acceso del host D143	43
Ilustración 30 configuración puertos de acceso del host A144	44
Ilustración 31 DHCP IPv4 en PC244	44
Ilustración 32 DHCP IPv4 en PC345	45
Ilustración 33 Condiciones de conectividad PC145	45
Ilustración 34 Condiciones de conectividad PC246	46
Ilustración 35 configuración single-area OSPFv2 en area 0 en R149	49
Ilustración 36 configuración single-area OSPFv2 en area 0 en R350	50
Ilustración 37 configuración single-area OSPFv2 en area 0 en D1.....51	51
Ilustración 38 configuración single-area OSPFv2 en area 0 en D2.....52	52
Ilustración 39 configuración classic single-area OSPFv3 en area 0 en R153	53
Ilustración 40 configuración classic single-area OSPFv3 en area 0 en R354	54
Ilustración 41 configuración classic single-area OSPFv3 en area 0 en D155	55

Ilustración 42 configuración classic single-area OSPFv3 en area 0 en D2	56
Ilustración 43 configuración MP-BGP en R2	57
Ilustración 44 configuración MP-BGP en R1	58
Ilustración 45 accesibilidad de la interfaz R1 G0/0/1	61
Ilustración 46 cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1	62
Ilustración 47 Grupo 104 vlan 100	63
Ilustración 48 Grupo 114 Vlan 101	64
Ilustración 49 Grupo 124 vlan 102.	64
Ilustración 50 Grupo 106 vlan 100	65
Ilustración 51 Grupo 116 Vlan 101.	66
Ilustración 52 Grupo 126 vlan 102	66
Ilustración 53 Grupo 104 vlan 100	67
Ilustración 54 Grupo 126 vlan 102	68
Ilustración 55 proteja el EXEC privilegiado usando el algoritmo de inscripción SCRYPT	69

GLOSARIO

Conmutador (switch): es un dispositivo de enlace que realiza un puente entre múltiples puertos, tiene las propiedades de actuar eficientemente como dispositivo de capa de enlace de datos. Dentro de sus funciones este elemento de la red realiza una verificación de errores antes de reenviar paquetes. divide el dominio de colisión de los hosts, pero el dominio de difusión sigue siendo el mismo.

Enrutadores (Router): estos elementos son dispositivos con la propiedad de enlazar dos o más redes diferentes, dentro de su estructura se pueden componer de diferentes tipos de segmentos de red LAN. Este dispositivo, recibe paquetes de datos y selecciona dentro de una tabla la ruta más eficaz para reenviar el paquete a través de la red. La tabla es llamada tabla de enrutamiento y es creada por el mismo dispositivo, estos dispositivos operan en el nivel de capa de red del modelo IOS.

Protocolos: los protocolos de enrutamiento administran la actividad de enrutamiento en un sistema, Estos protocolos son un conjunto de reglas utiliza un router cuando se comunica con otros router con el fin de compartir y sincronizar información de enrutamiento. La finalidad es mantener la información actualizada para construir las tablas de enrutamiento.

Etherchannel: Es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad. Los puertos usados deben tener las mismas características y configuración.

RESUMEN

El aprendizaje y conocimientos básicos de computación y redes son elementos necesarios en el campo de trabajo de un profesional en tecnologías, por esta razón el conocimiento en redes y comunicaciones forman uno de los principales pilares del conocimiento técnico, la necesidad de acceder al diplomado en CCNP tiene como principal finalidad el desarrollo de competencias que me permitan abordar desafíos en el mundo moderno, proyectos que parten basados en la construcción, evolución y reparación de redes informáticas, los conocimientos que nos ofrece la academia de aprendizaje CISCO con sus programas a través de la Universidad Nacional Abierta y a Distancia nos permiten lograr este objetivo.

Los sistemas informáticos están presentes en todos los entornos tecnológicos modernos y gracias a ellos son una gran oportunidad de incursión de nuestra vida profesional. La economía global gira entorno a redes informáticas, los sistemas productivos avanzan alrededor basados en redes, hemos pasado de equipos que operaban en un gran porcentaje con intervención humana a equipos que tienen la capacidad de analizar y evaluar tareas basados en aprendizaje para ejecutar procesos y que pueden comunicarse con otros equipos ubicados a grandes distancias incluso fuera de nuestro planeta.

La certificación en CISCO es una gran oportunidad de incursión en el mercado de las comunicaciones y transporte de datos, la gran mayoría de arquitecturas operan bajo su tecnología.

Palabras Claves: Conmutación, CCNP, Enrutamiento, CISCO, Redes, Datos, Tecnologías, Protocolos, informática.

ABSTRACT

Learning and basic knowledge of computing and networks are necessary elements in the field of work of a professional in technologies, for this reason knowledge in networks and communications form one of the main pillars of technical knowledge, the need to access the diploma in CCNP Its main purpose is the development of competencies that allow me to address challenges in the modern world, projects that start based on the construction, evolution and repair of computer networks, the knowledge offered by the CISCO learning academy with its programs through the National Open and Distance University allow us to achieve this objective.

Computer systems are present in all modern technological environments and thanks to them they are a great opportunity to foray into our professional life. The global economy revolves around computer networks, productive systems move around based on networks, we have gone from teams that operated in a large percentage with human intervention to teams that have the ability to analyze and evaluate tasks based on learning to execute processes and that they can communicate with other equipment located at great distances even outside our planet.

Certification in CISCO is a great opportunity to enter the communications and data transport market, the vast majority of architectures operate under its technology.

Keywords: Switching, CCNP, Routing, CISCO, Networks, Data, Technologies, Protocols, computing..

INTRODUCCION

El mundo moderno y la sociedad actual requieren de persona con capacidades técnicas y tecnologías que permitan la construcción segura de redes y centros informáticos dedicados al resguardo eh intercambio de información. En todos los casos esta información se debe mantener bajo resguardo y con protección de un administrador, lejos de manos de personas o grupos que la puedan utilizar para generar daño. El diplomado de CISCO nos brinda esta oportunidad.

A lo largo del desarrollo de este taller de evaluación de conocimientos nos encontraremos con elementos de aprendizaje que abarcan desde el ámbito de interacción de un software de simulación de redes como es el PACKET TRACER, la construcción de una red dentro de su entorno de simulación y la configuración lógica de dispositivos como swich, routers y terminales, todo bajo el concepto de una red segura, eficiente, estable y lógica.

Para lograr el objetivo de una red con las características mencionadas anteriormente, se requiere del conocimiento básicos y avanzado en formulación de instrucciones y comandos que realicen las tareas requeridas, gran parte del conocimiento es la capacidad de asesoramiento a un cliente sobre los equipos más eficientes a su necesidad que le implique una inversión baja sin dejar de lado los conceptos anteriores, almacenamiento seguro, transporte rápido eficiente, estable y seguro.

La estabilidad de la red es una de las principales características que se debe ofrecer a un cliente, las diferentes configuraciones físicas en conjunto con los comandos a trabajar dentro de este ejercicio de evaluación nos permitirán cumplir este requerimiento. Sería muy molesto que nos encontráramos en una transacción importante muy delicada donde esté en juego una gran inversión y nuestro sistema colapsara continuamente. Este ejercicio nos permitirá darle la robustes que se requiere ante posibles fallos

DESARROLLO

1. ESCENARIO 1

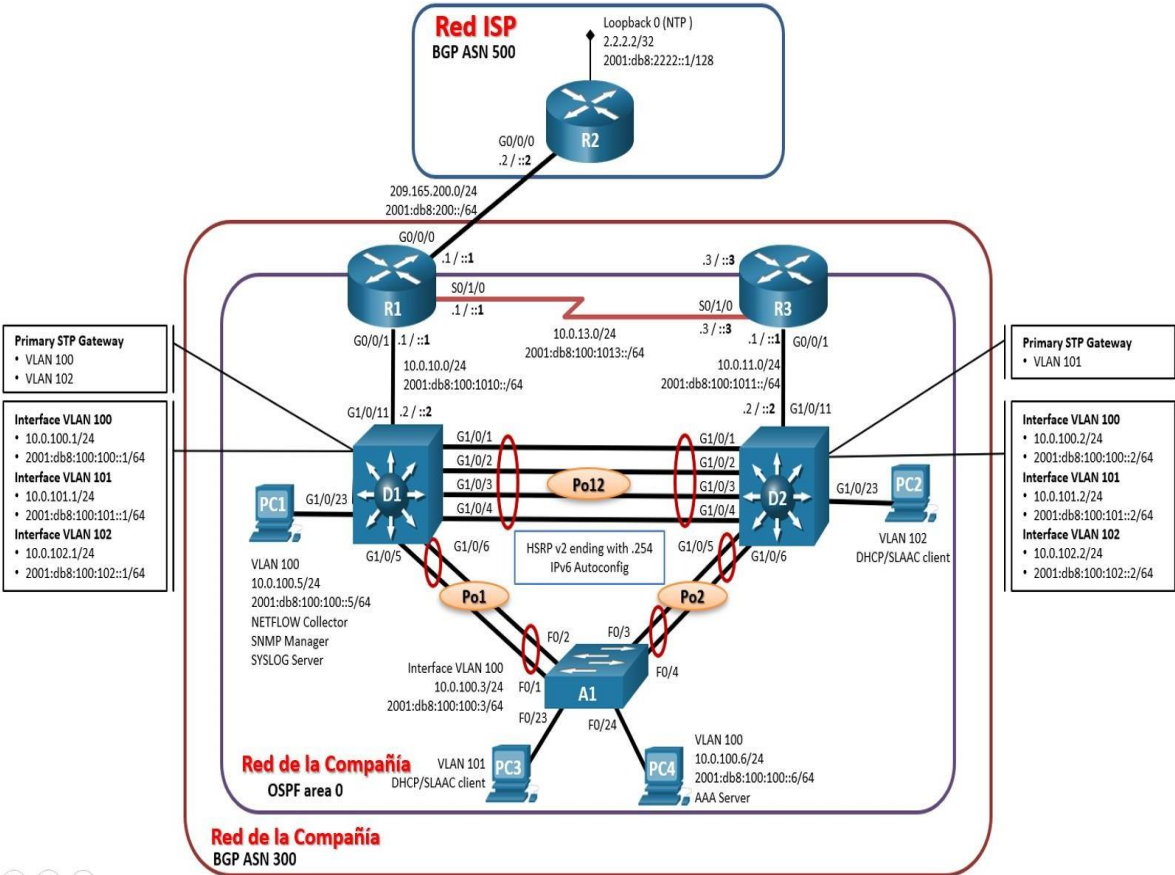


Ilustración 1 Topología de Red

Tabla 1 Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

OBJETIVOS

Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

Part 2: Configurar la capa 2 de la red y el soporte de Host

Part 3: Configurar los protocolos de enrutamiento

Part 4: Configurar la redundancia del primer salto

Part 5: Configurar la seguridad

Part 6: Configurar las características de administración de red

ESCENARIO

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "**Red de la Compañía**" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Nota: Los routers usados son Cisco 4221 con CISCO IOS XE versión 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE versión 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS versión 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.

Nota: Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tengan configuraciones de inicio.

Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global `sdm prefer dual-ipv4-and-ipv6 default`. Cambiar la plantilla requerirá el reinicio del switch.

Recursos necesarios

- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
- 4 PCs (utilice el programa de emulación de terminal)
- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola
- Los cables Ethernet y seriales van como se muestra en la topología

Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

Paso 1: Cablear la red como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

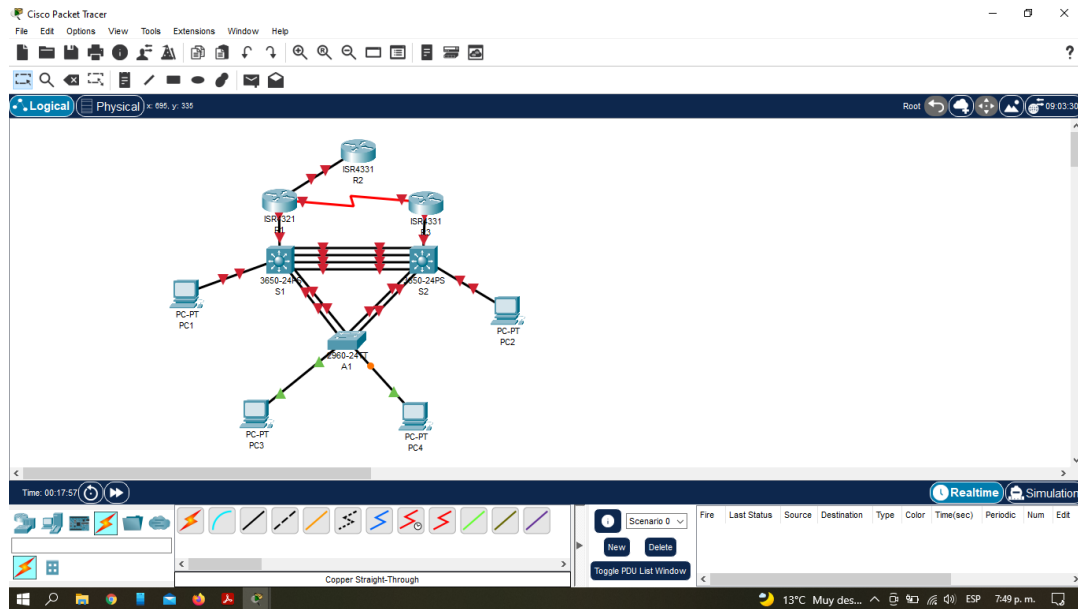


Ilustración 2 Modelo distribución de red y conexasiónado

Paso 2: Configurar los parámetros básicos para cada dispositivo.

- a. Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

Router R1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
  exec-timeout 0 0
  logging synchronous
  exit
interface g0/0/0
  ip address 209.165.200.225 255.255.255.224
  ipv6 address fe80::1:1 link-local
  ipv6 address 2001:db8:200::1/64
  no shutdown
  exit
interface g0/0/1
  ip address 10.0.10.1 255.255.255.0
  ipv6 address fe80::1:2 link-local
  ipv6 address 2001:db8:100:1010::1/64
  no shutdown
  exit
```

```

interface s0/1/0
  ip address 10.0.13.1 255.255.255.0
  ipv6 address fe80::1:3 link-local
  ipv6 address 2001:db8:100:1013::1/64
  no shutdown
exit

```

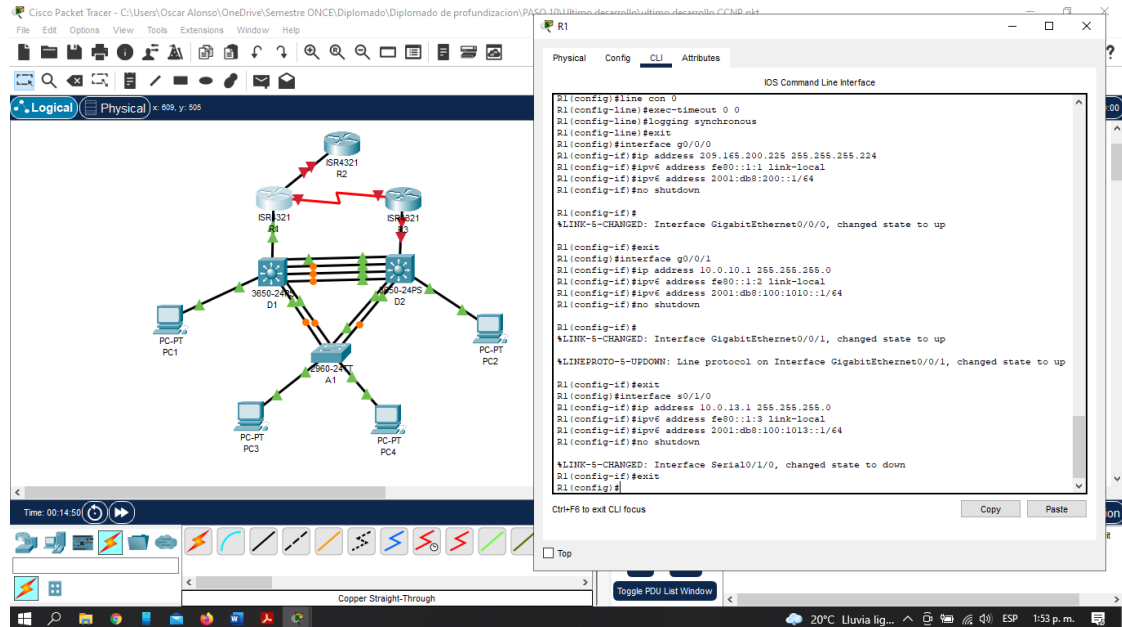


Ilustración 3 Configuración inicial Router R1

Router R2

```

hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
  exec-timeout 0 0
  logging synchronous
  exit
interface g0/0/0
  ip address 209.165.200.226 255.255.255.224
  ipv6 address fe80::2:1 link-local
  ipv6 address 2001:db8:200::2/64
  no shutdown
  exit
interface Loopback 0
  ip address 2.2.2.2 255.255.255.255
  ipv6 address fe80::2:3 link-local
  ipv6 address 2001:db8:2222::1/128
  no shutdown

```

exit

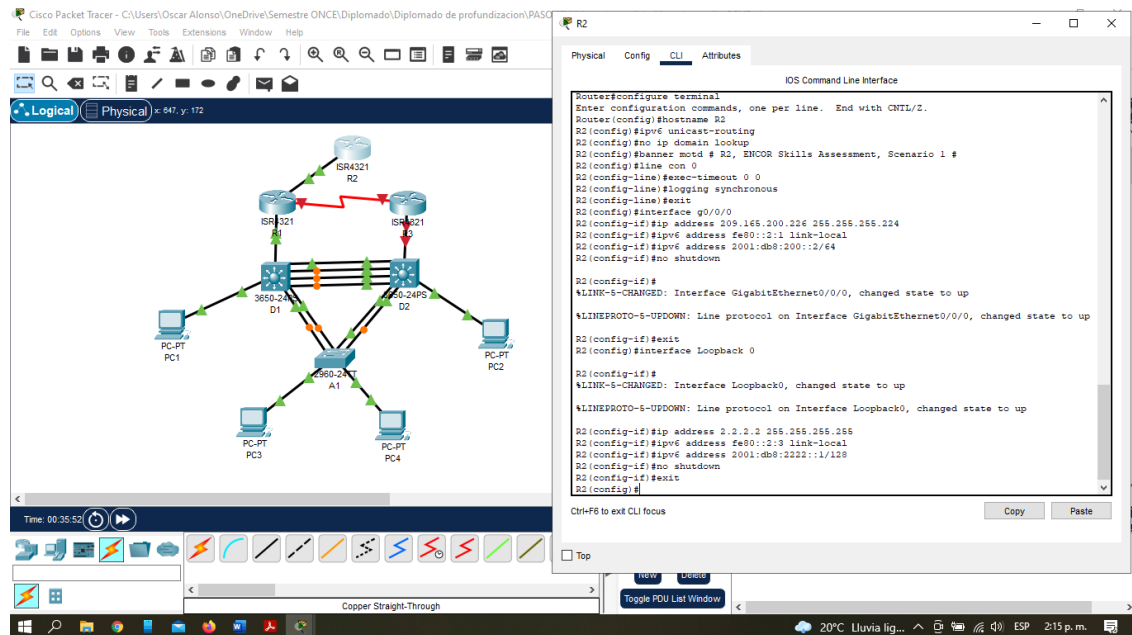


Ilustración 4 Configuración inicial Router R2

Router R3

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
  exec-timeout 0 0
  logging synchronous
  exit
interface g0/0/1
  ip address 10.0.11.1 255.255.255.0
  ipv6 address fe80::3:2 link-local
  ipv6 address 2001:db8:100:1011::1/64
  no shutdown
  exit
interface s0/1/0
  ip address 10.0.13.3 255.255.255.0
  ipv6 address fe80::3:3 link-local
  ipv6 address 2001:db8:100:1010::2/64
  no shutdown
  exit
```

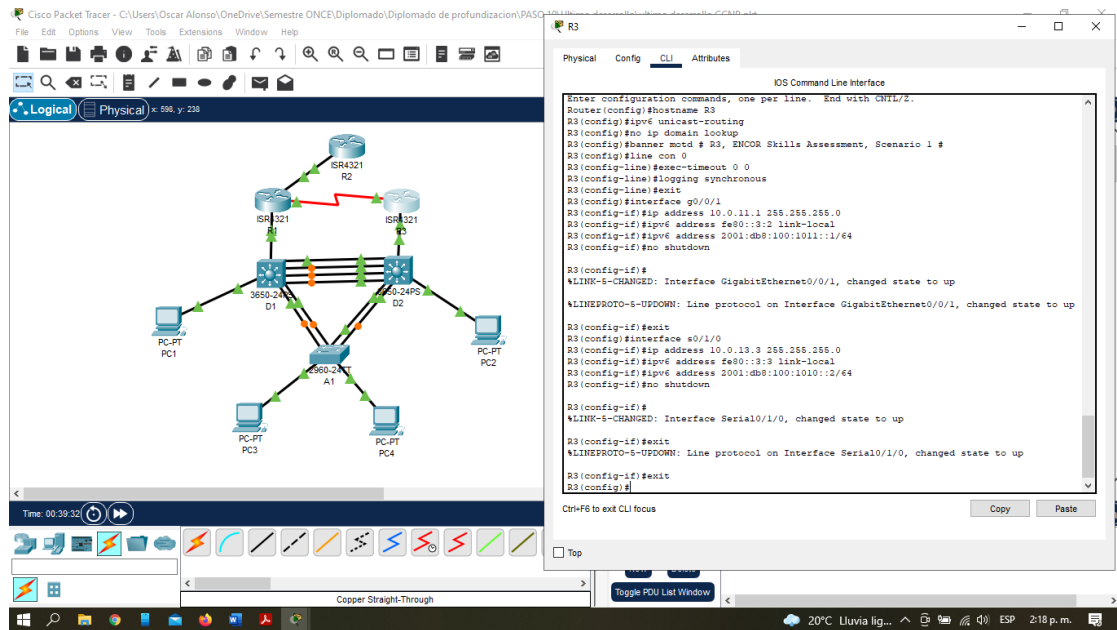


Ilustración 5 Configuración inicial Router R3

Switch D1

```

hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
    exec-timeout 0 0
    logging synchronous
    exit
vlan 100
    name Management
    exit
vlan 101
    name UserGroupA
    exit
vlan 102
    name UserGroupB
    exit
vlan 999
    name NATIVE
    exit
interface g1/0/11
    no switchport
    ip address 10.0.10.2 255.255.255.0
    ipv6 address fe80::d1:1 link-local
    ipv6 address 2001:db8:100:1010::2/64

```

```
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

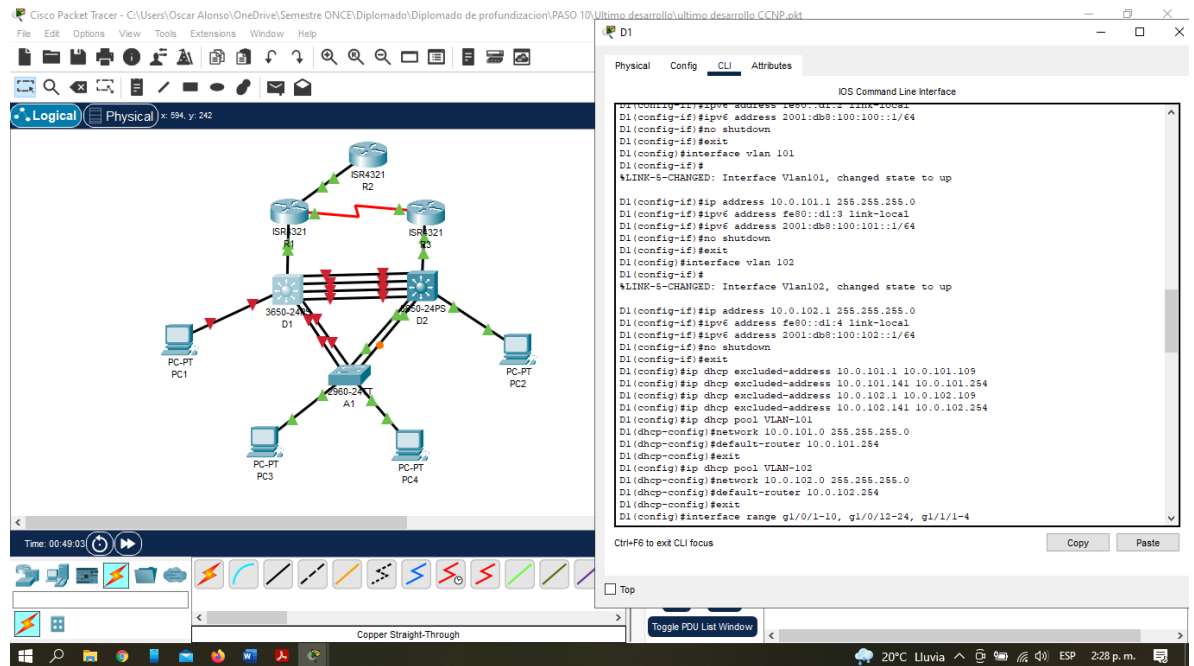


Ilustración 6 Configuración inicial Switch D1

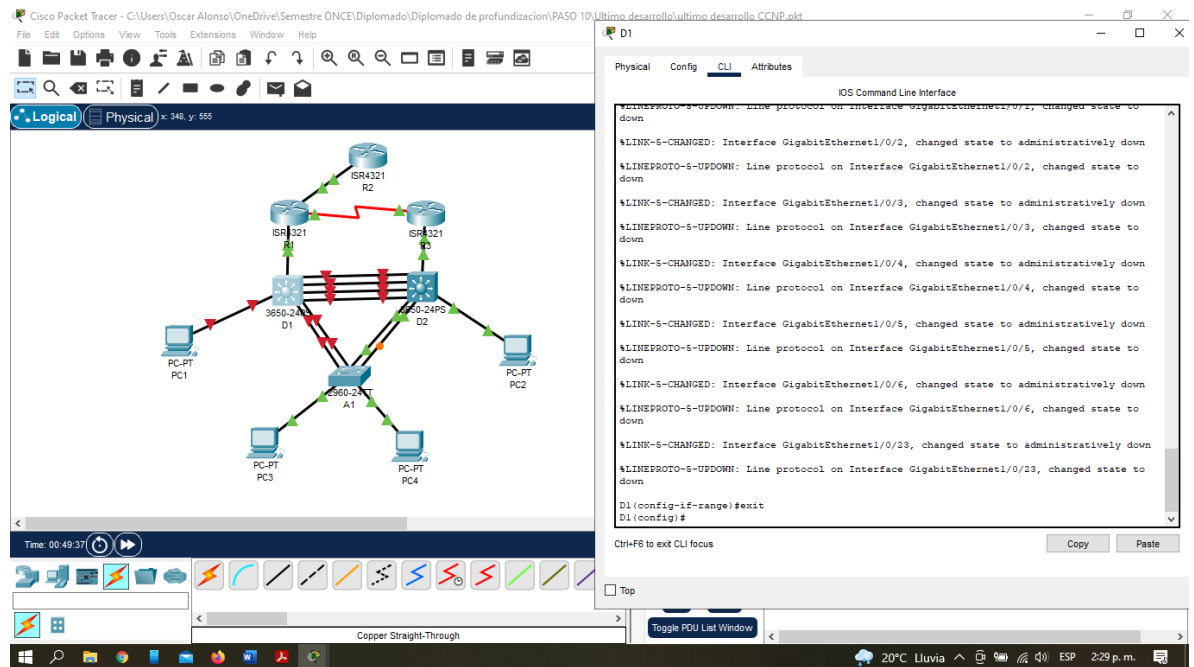


Ilustración 7 Configuración inicial Switch D2

Switch D2

```

hostname D2
ip routing
ipv6 unicast-routing

```

```
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
    exec-timeout 0 0
    logging synchronous
    exit
vlan 100
    name Management
    exit
vlan 101
    name UserGroupA
    exit
vlan 102
    name UserGroupB
    exit
vlan 999
    name NATIVE
    exit
interface g1/0/11
    no switchport
    ip address 10.0.11.2 255.255.255.0
    ipv6 address fe80::d1:1 link-local
    ipv6 address 2001:db8:100:1011::2/64
    no shutdown
    exit
interface vlan 100
    ip address 10.0.100.2 255.255.255.0
    ipv6 address fe80::d2:2 link-local
    ipv6 address 2001:db8:100:100::2/64
    no shutdown
    exit
interface vlan 101
    ip address 10.0.101.2 255.255.255.0
    ipv6 address fe80::d2:3 link-local
    ipv6 address 2001:db8:100:101::2/64
    no shutdown
    exit
interface vlan 102
    ip address 10.0.102.2 255.255.255.0
    ipv6 address fe80::d2:4 link-local
    ipv6 address 2001:db8:100:102::2/64
    no shutdown
    exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
    network 10.0.101.0 255.255.255.0
    default-router 10.0.101.254
```

```

exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit

```

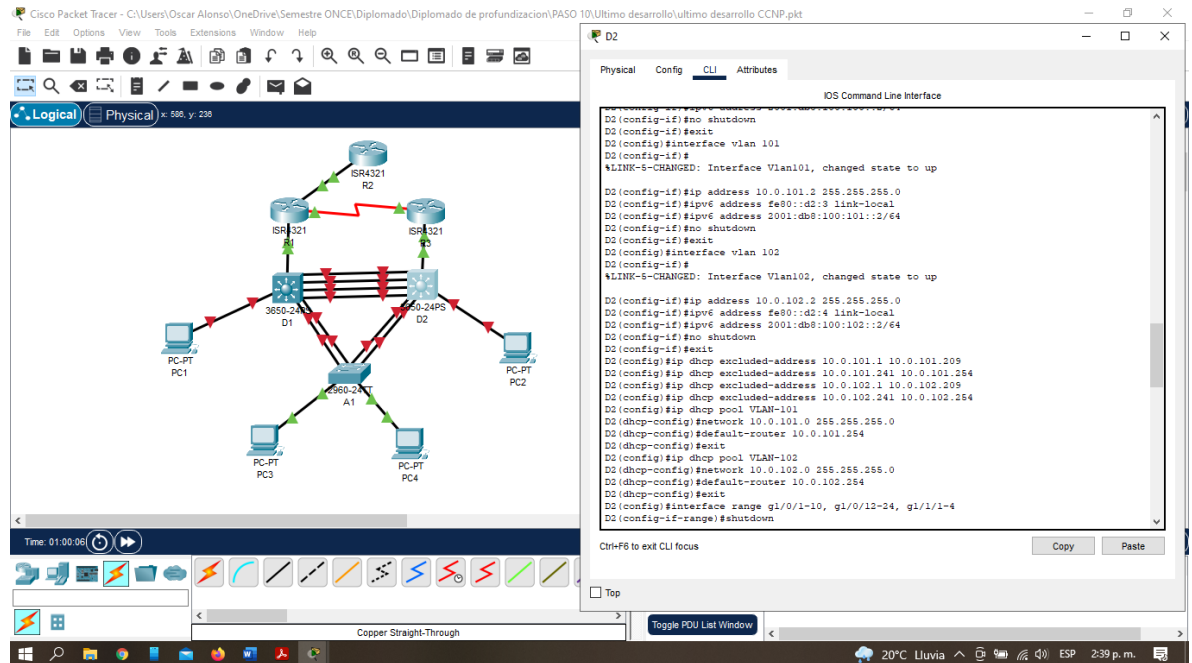


Ilustración 8 Configuración inicial Switch D2

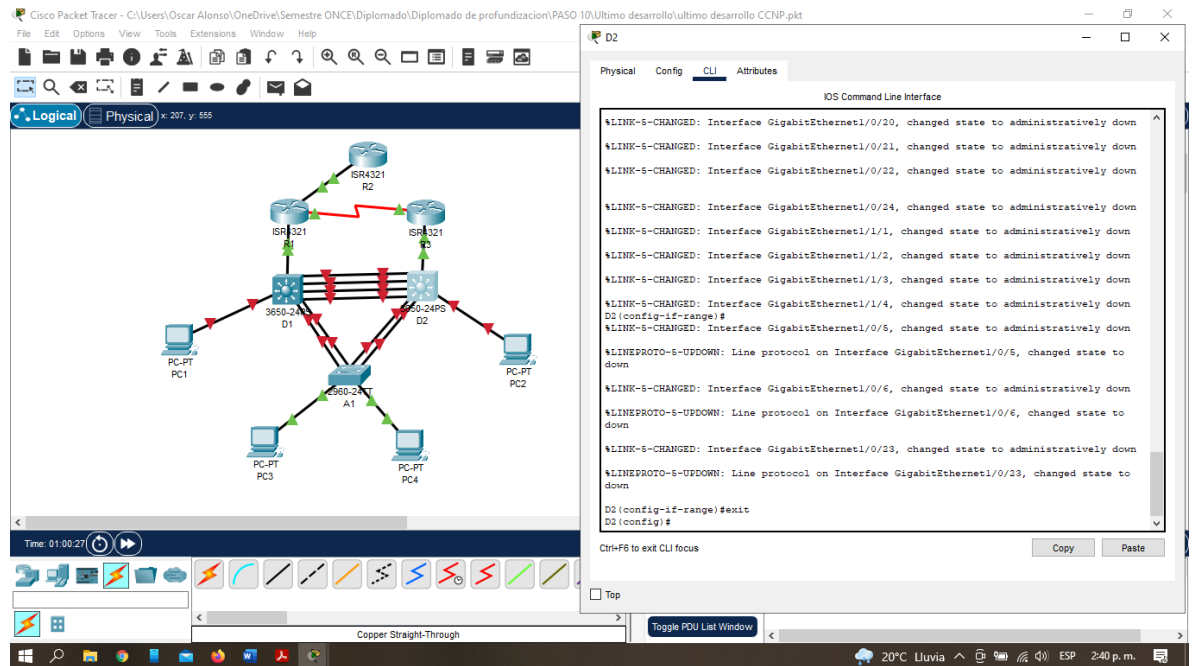


Ilustración 9 Configuración inicial Switch D2

Switch A1

```

hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
  exec-timeout 0 0
  logging synchronous
  exit
vlan 100
  name Management
  exit
vlan 101
  name UserGroupA
  exit
vlan 102
  name UserGroupB
  exit
vlan 999
  name NATIVE
  exit
interface vlan 100
  ip address 10.0.100.3 255.255.255.0
  ipv6 address fe80::a1:1 link-local
  ipv6 address 2001:db8:100:100::3/64
  no shutdown
  exit
  
```

```

interface range f0/5-22
shutdown
exit

```

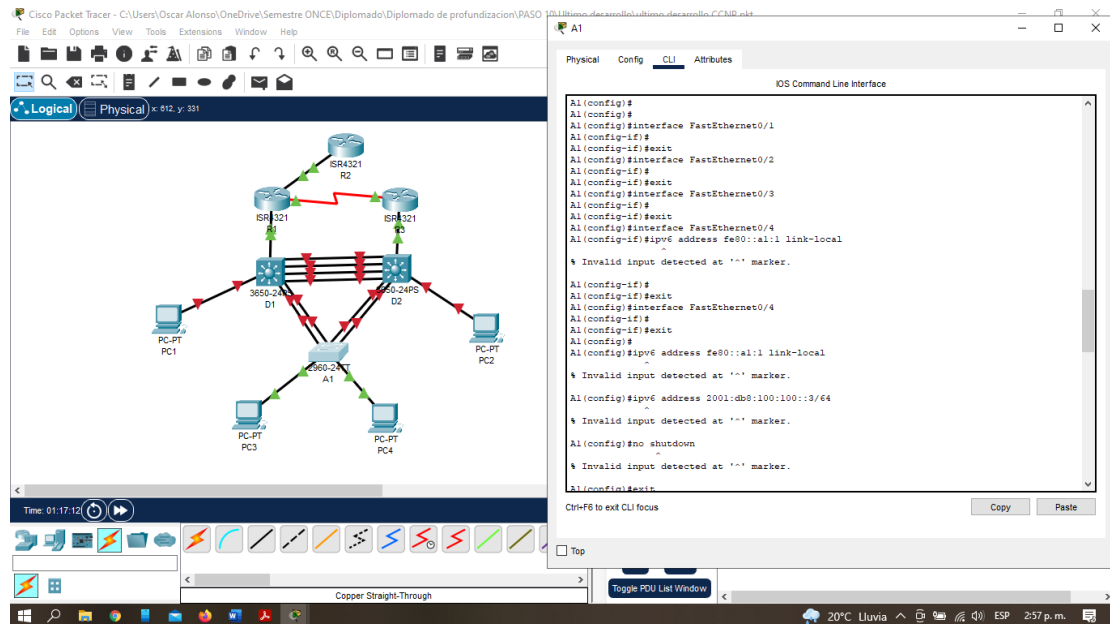


Ilustración 10 Configuración inicial Switch A1

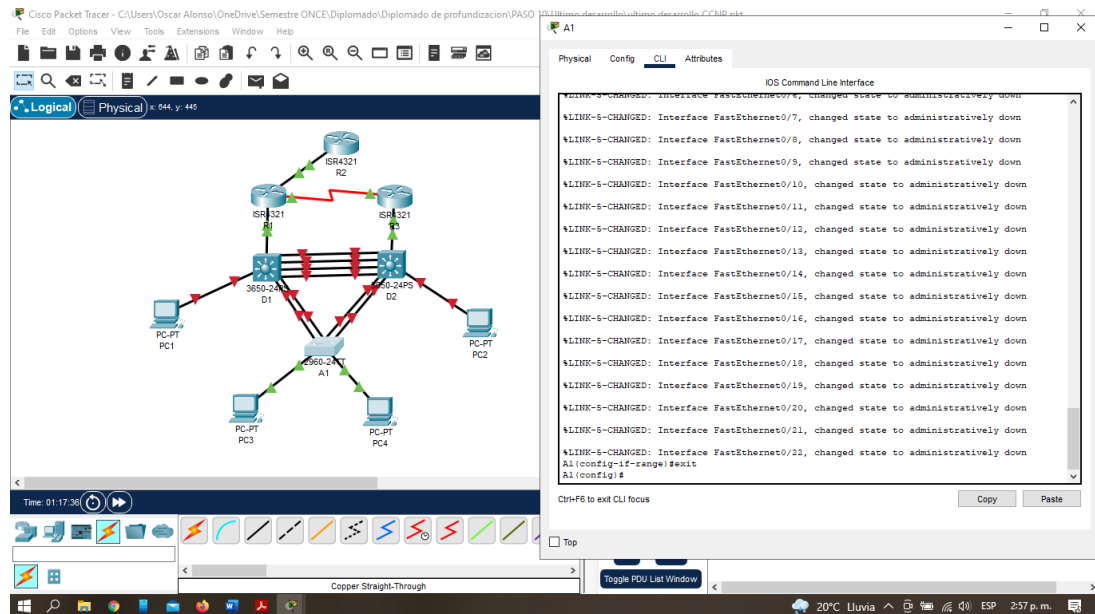


Ilustración 11 Configuración inicial Switch A1

- Copie el archivo **running-config** al archivo **startup-config** en todos los dispositivos.
- Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

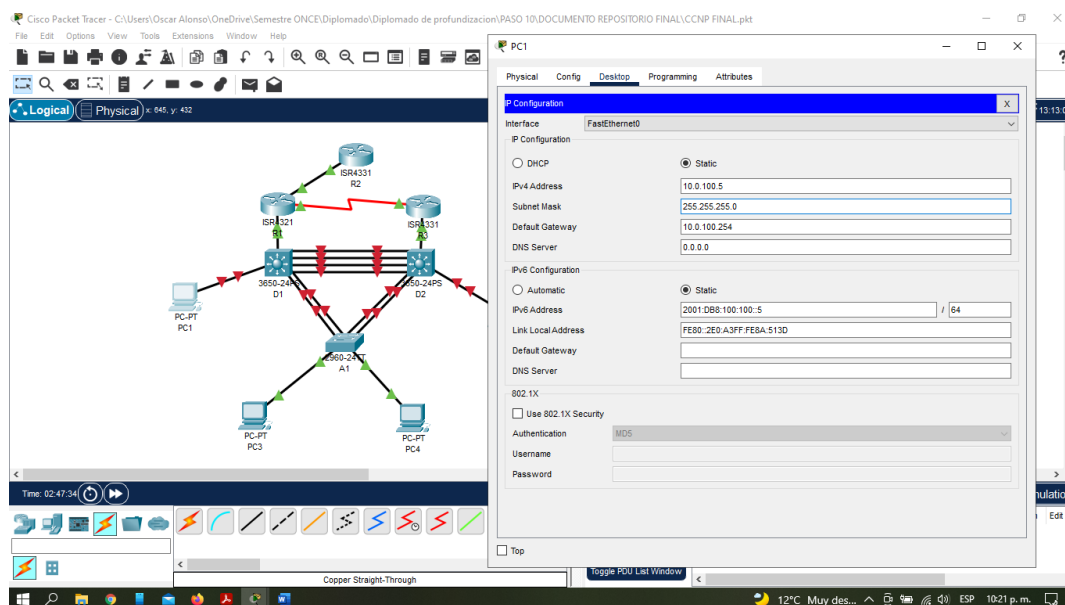


Ilustración 12 Configuración inicial PC1

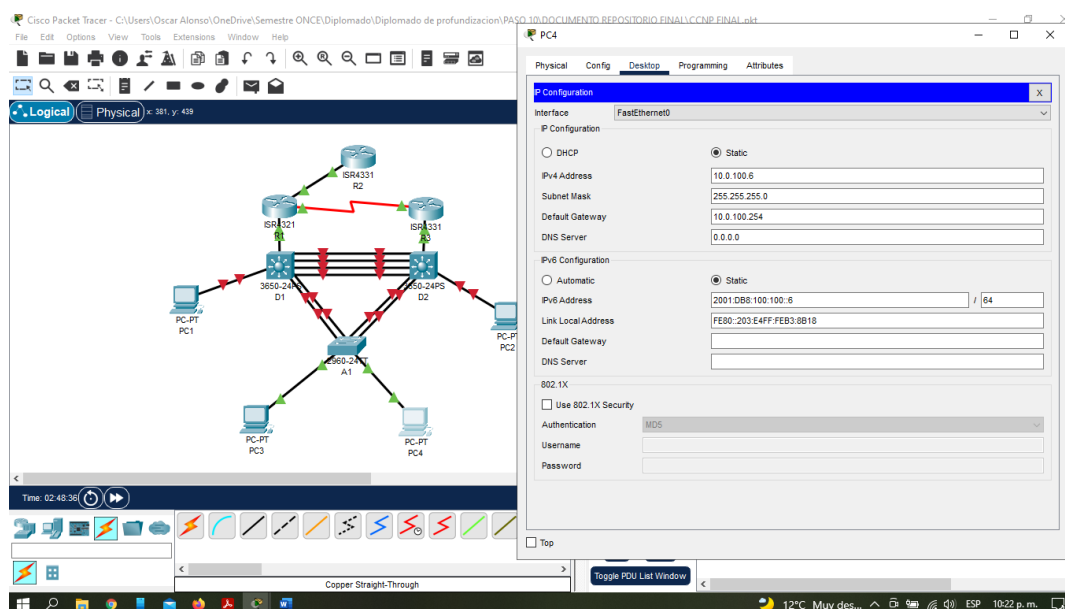


Ilustración 13 configuración inicial PC2

2 Parte 2: Configurar la capa 2 de la red y el soporte de Host

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC. Las tareas de configuración son las siguientes:

Tabla 2 Configurar la capa 2 de la red y el soporte de Host

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.101.1

		<ul style="list-style-type: none"> • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 PC1: 10.0.100.5
--	--	---

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Configuración Switch D1

```

D1(config)#inter g1/0/1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#inter g1/0/2
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#inter g1/0/3
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#inter g1/0/4
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#inter g1/0/5
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#inter g1/0/6
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk

```

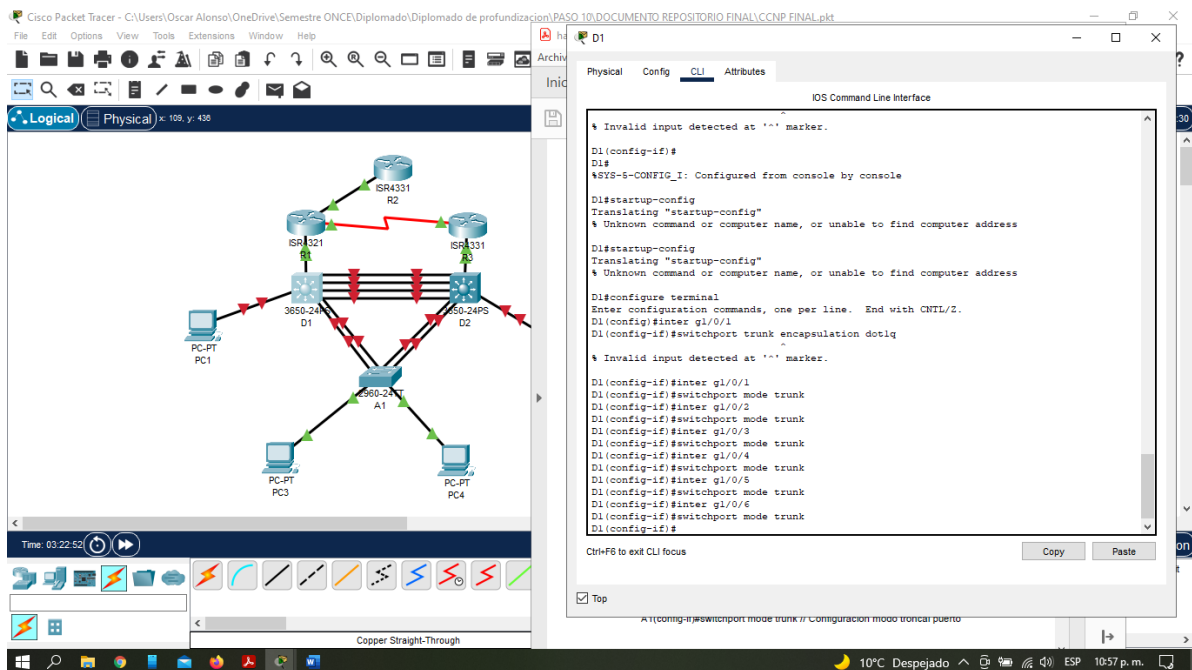


Ilustración 14 configuración interfaces troncales IEEE 802.1Q Switch D1

Configuración Switch D2

```

D2(config)#interface g1/0/1
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#interface g1/0/2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#interface g1/0/3
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#interface g1/0/4
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#interface g1/0/5
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#interface g1/0/6
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
  
```

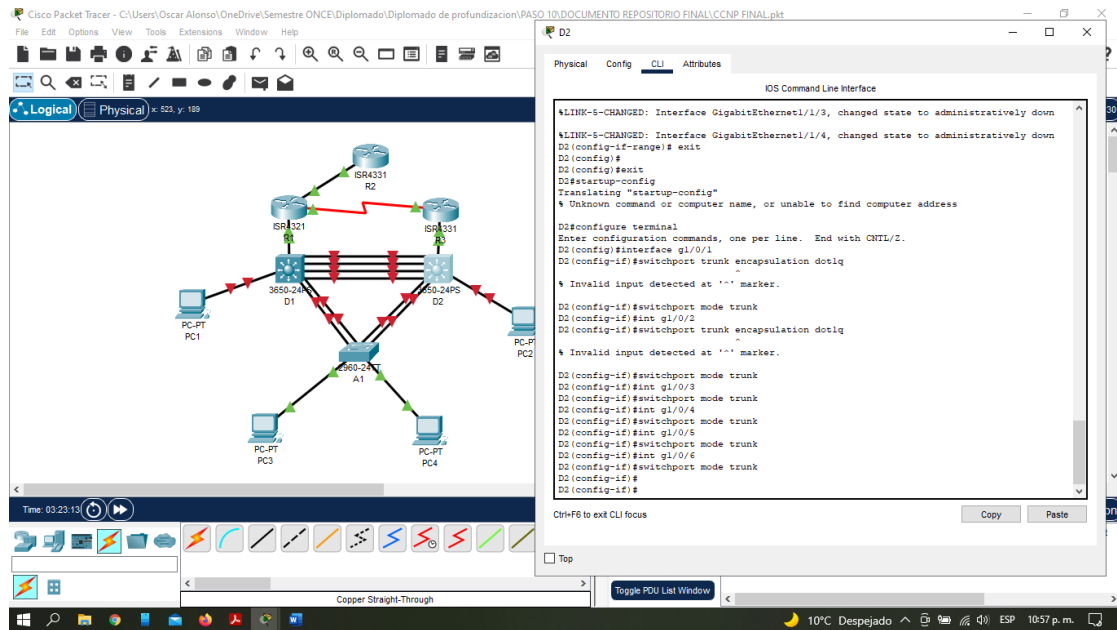
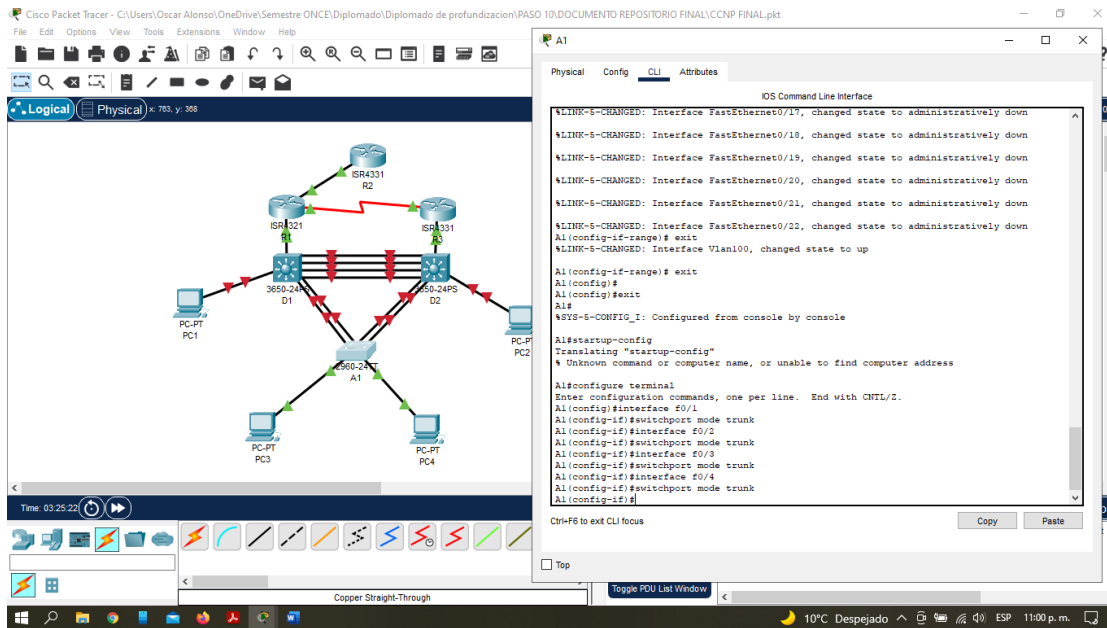


Ilustración 15 configuración interfaces troncales IEEE 802.1Q Switch D2

Configuración Switch A1

```

A1(config)#interface f0/1
A1(config-if)#switchport mode trunk
A1(config-if)#interface f0/2
A1(config-if)#switchport mode trunk
A1(config-if)#interface f0/3
A1(config-if)#switchport mode trunk
A1(config-if)#interface f0/4
A1(config-if)#switchport mode trunk
A1(config-if)#
  
```



2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

Configuración Switch D1

```
D1(config)#interface g1/0/1
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#interface g1/0/2
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#interface g1/0/3
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#interface g1/0/4
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#interface g1/0/5
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#interface g1/0/6
D1(config-if)#switchport trunk native vlan 999
```

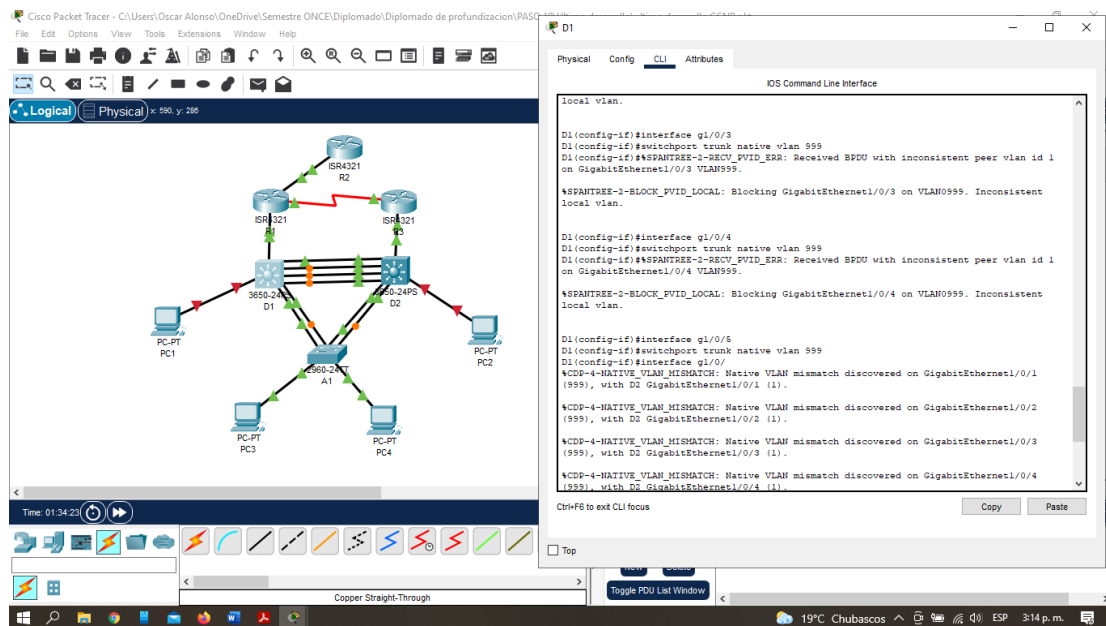



Ilustración 17 cambio la VLAN nativa en los enlaces troncales D1

Configuración Switch D1

```
D2(config)#interface g1/0/1
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#interface g1/0/2
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#interface g1/0/3
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#interface g1/0/4
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#interface g1/0/5
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#interface g1/0/6
D2(config-if)#switchport trunk native vlan 999
```

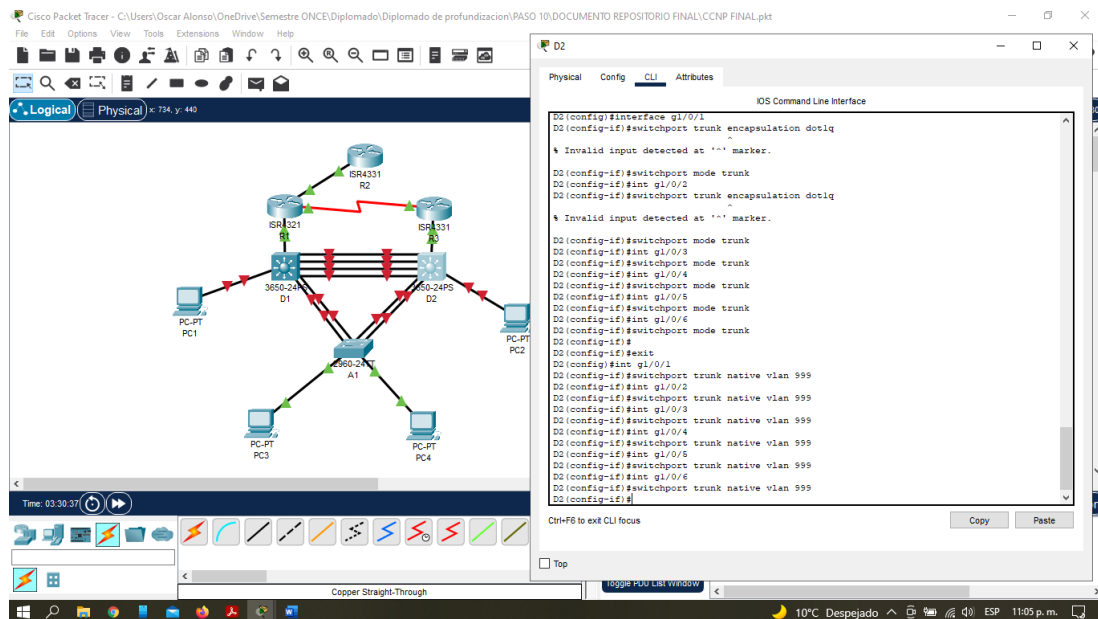


Ilustración 18 cambio la VLAN nativa en los enlaces troncales D2

Configuración Switch A1

```

A1(config-if)#interface f0/1
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#interface f0/2
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#interface f0/3
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#interface f0/4
A1(config-if)#switchport trunk native vlan 999
  
```

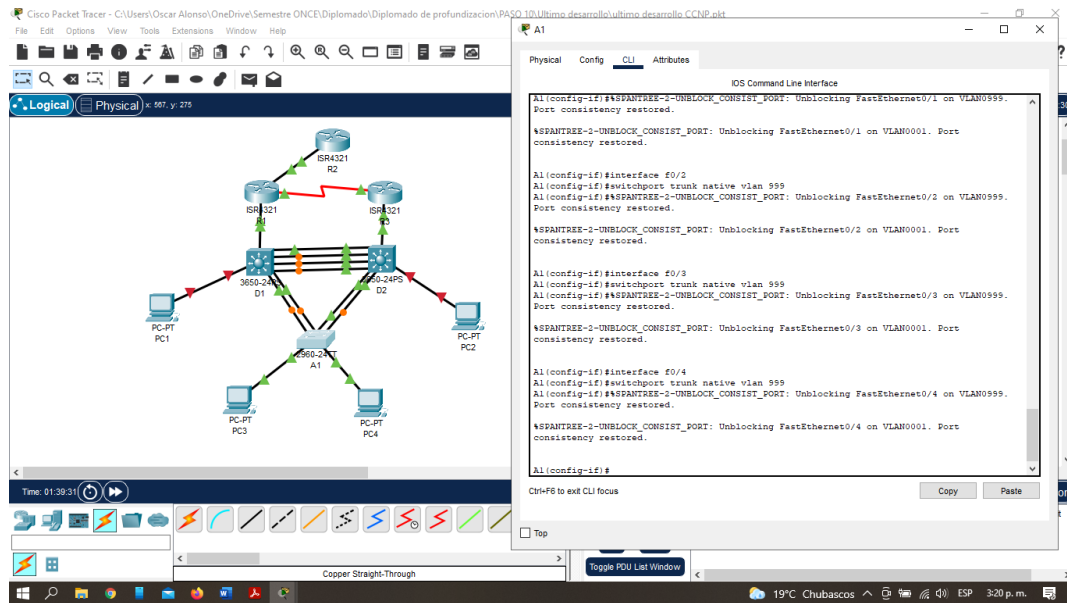


Ilustración 19 cambio la VLAN nativa en los enlaces troncales A1

2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

Configuración Switch D1

```
D1#configure termina
D1(config)#spanning-tree mode rapid-pvst
```

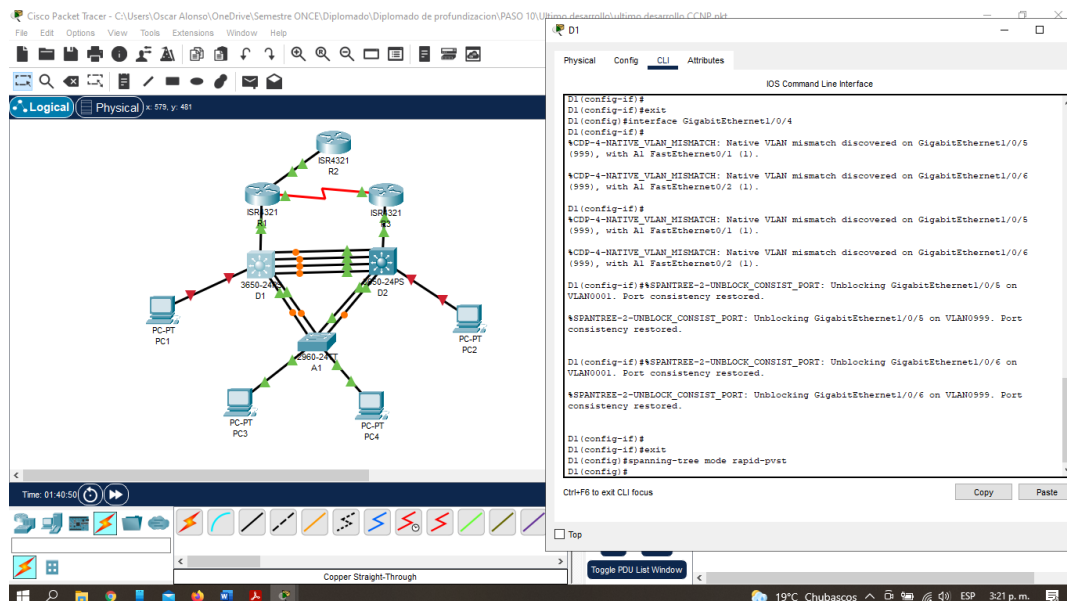


Ilustración 20 configuración rapid-pvst en D1

Configuración Switch D2

D2#configure termina

D2 (config)#spanning-tree mode rapid-pvst

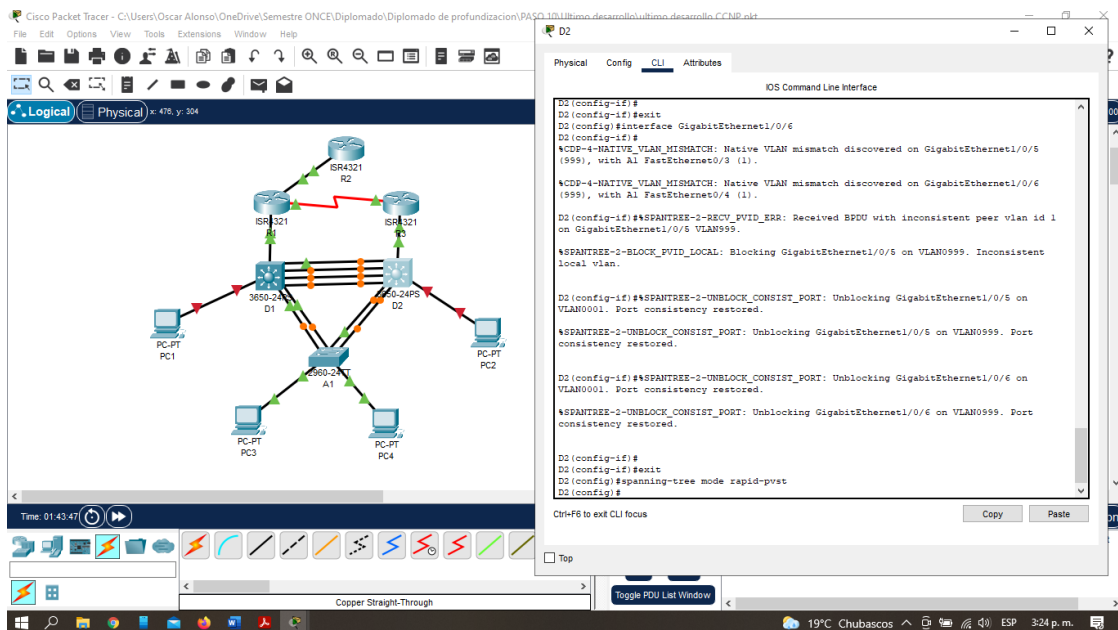
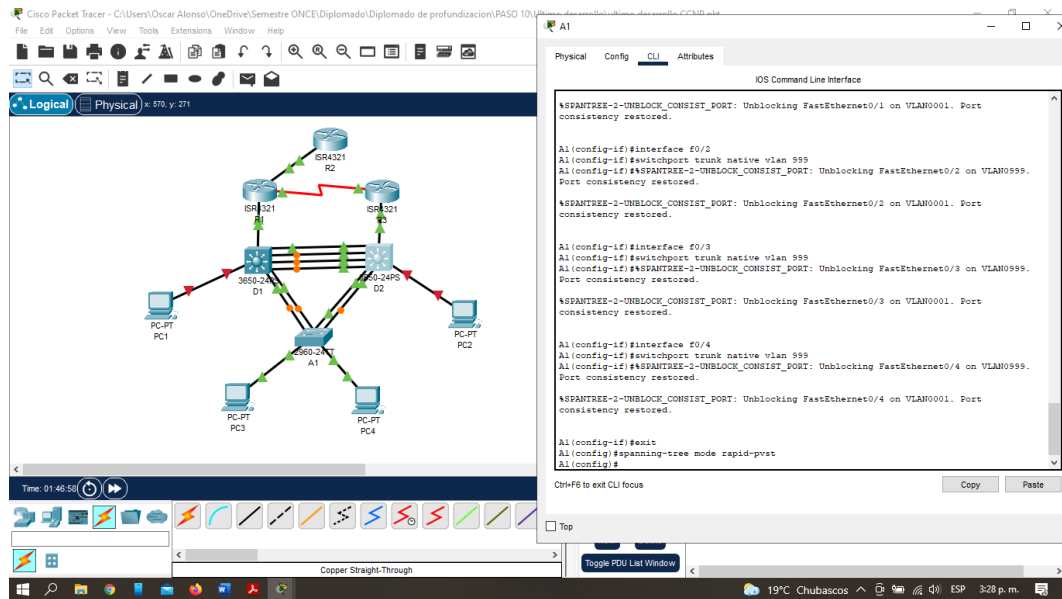


Ilustración 21 configuración rapid-pvst en D2

Configuración Switch A1

A1#configure termina

A1 (config)#spanning-tree mode rapid-pvst

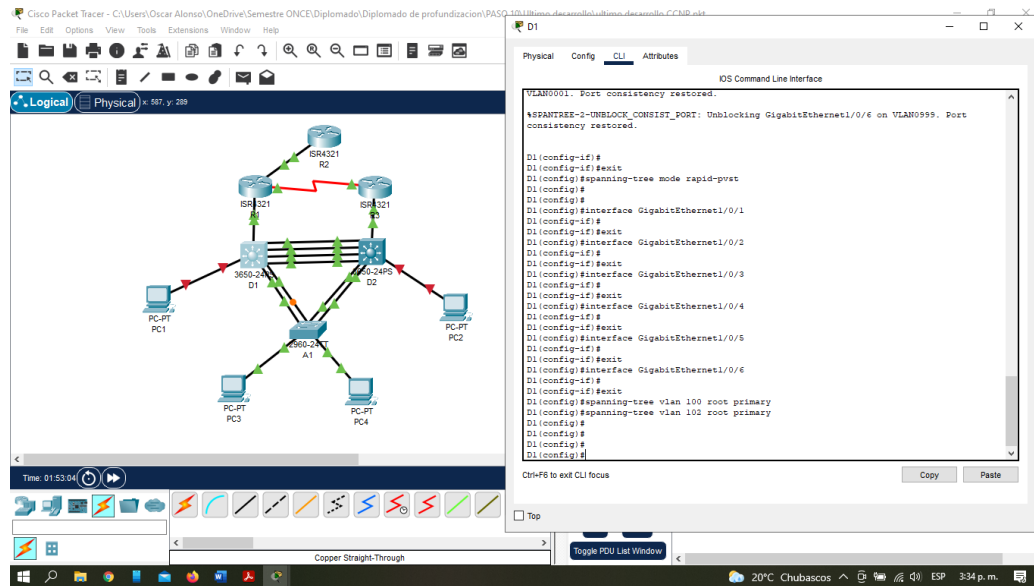


2.4 En D1 y D2, configure los puentes raíz RSTP(root bridges) según la información del diagrama de topología.

D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

Configuración Switch D1

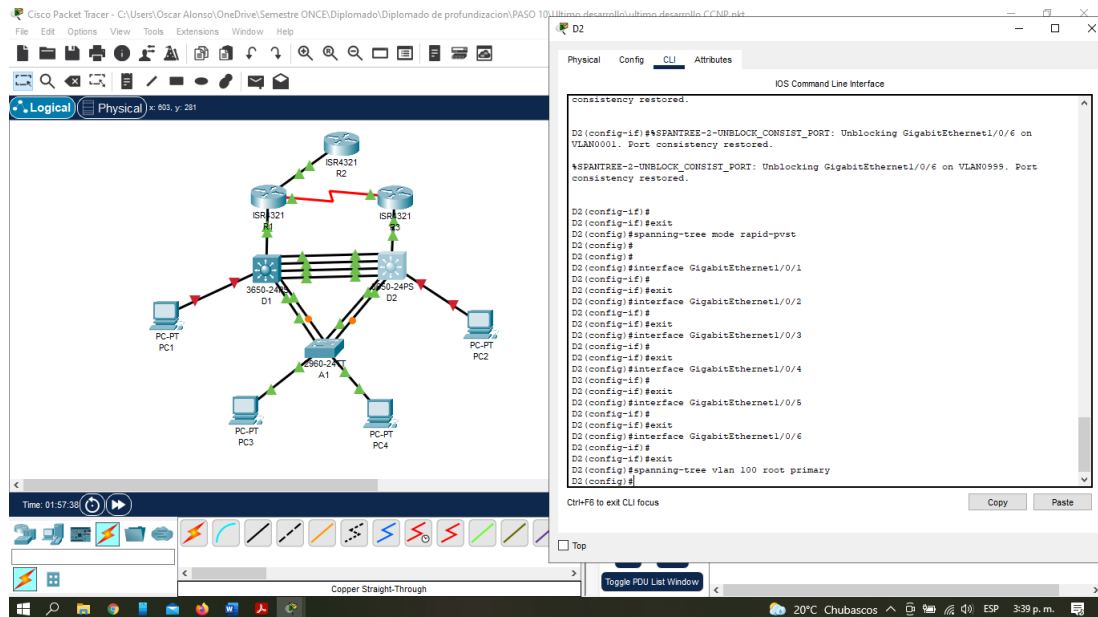
```
D1#conf terminal
D1(config)#spanning-tree vlan 100 root primary
D1(config)#spanning-tree vlan 102 root primary
```



Configuración Switch D2

```
D2#conf terminal
```

```
D2(config)#spanning-tree vlan 100 root primary
```



Configuración Switch D1

```
D1>enable
D1#configure terminal
D1(config)#interface range g1/0/1-4
D1(config-if-range)#switchport trunk native vlan 1
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 12
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#
D1(config)#interface range g1/0/5-6
D1(config-if-range)#switchport trunk native vlan 1
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 1
D1(config-if-range)#switchport trunk native vlan 999
```

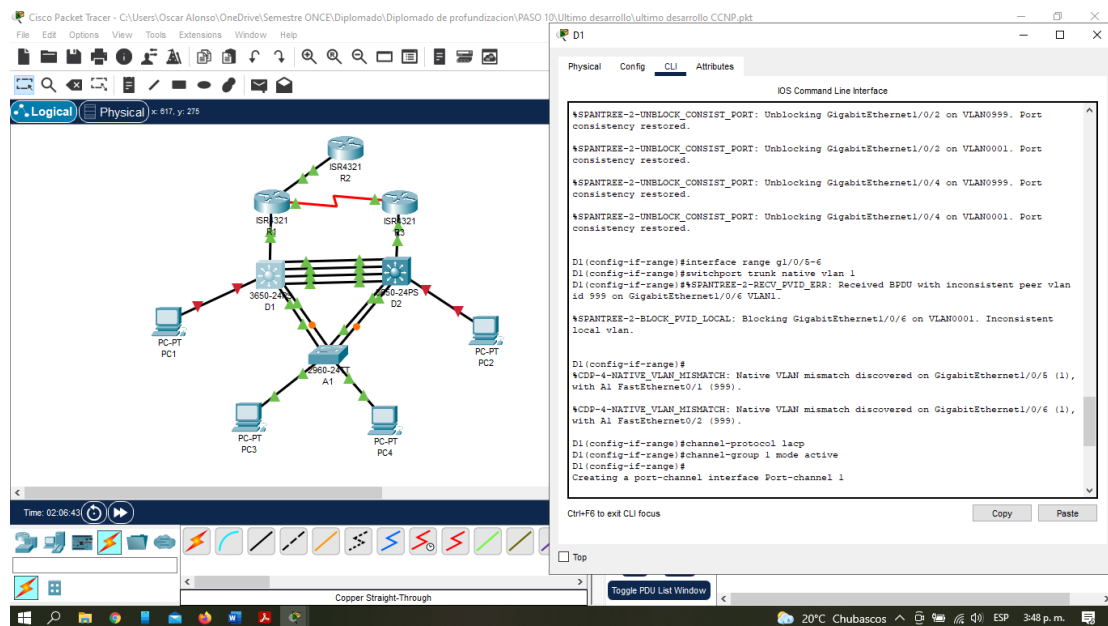


Ilustración 25 configuración EtherChannels LACP D1

Configuración Switch D2

```
D2>enable
D2#configure terminal
D2(config)#interface range g1/0/1-4
D2(config-if-range)#switchport trunk native vlan 1
```

```

D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#
Creating a port-channel interface Port-channel 12
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#
D2(config)#interface range g1/0/5-6
D2(config-if-range)#switchport trunk native vlan 1
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#
Creating a port-channel interface Port-channel 2
D2(config-if-range)#switchport trunk native vlan 999

```

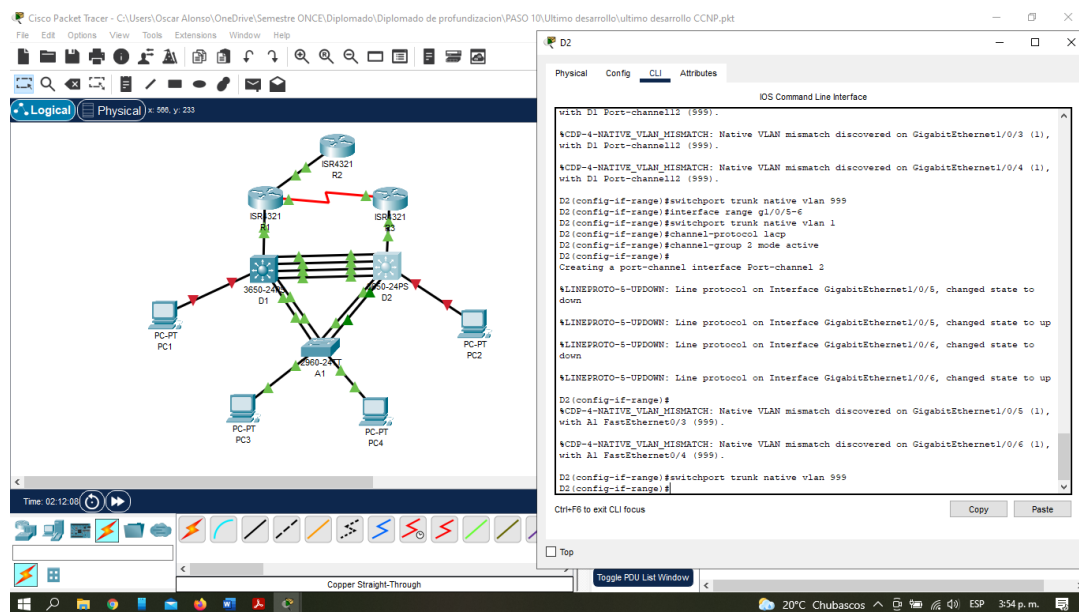


Ilustración 26 configuración EtherChannels LACP D2

Configuración Switch A1

```

A1#configure terminal
A1(config)#interface range f0/1-2
A1(config-if-range)#switchport trunk native vlan 1
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#
Creating a port-channel interface Port-channel 1
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#interface range f0/3-4
A1(config-if-range)#switchport trunk native vlan 1
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#

```



```

Creating a port-channel interface Port-channel 2
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#

```

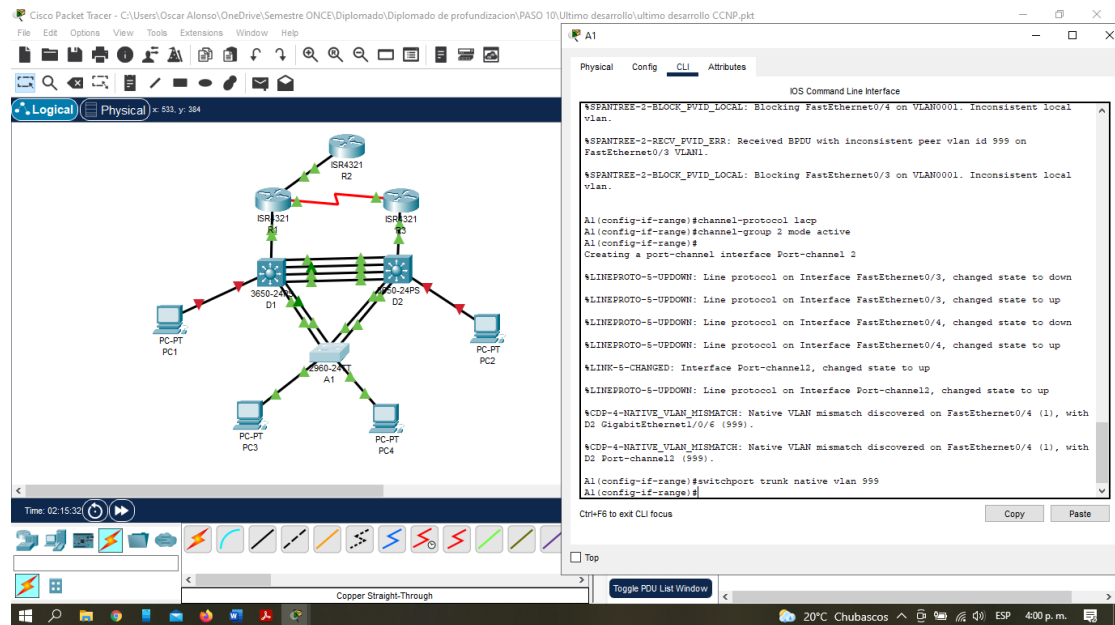


Ilustración 27 configuración EtherChannels LACP A1

2.6 En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

Configuración Switch D1

```

D1#configure terminal
D1(config)#interface g1/0/23
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100
D1(config-if)#no shutdown

```

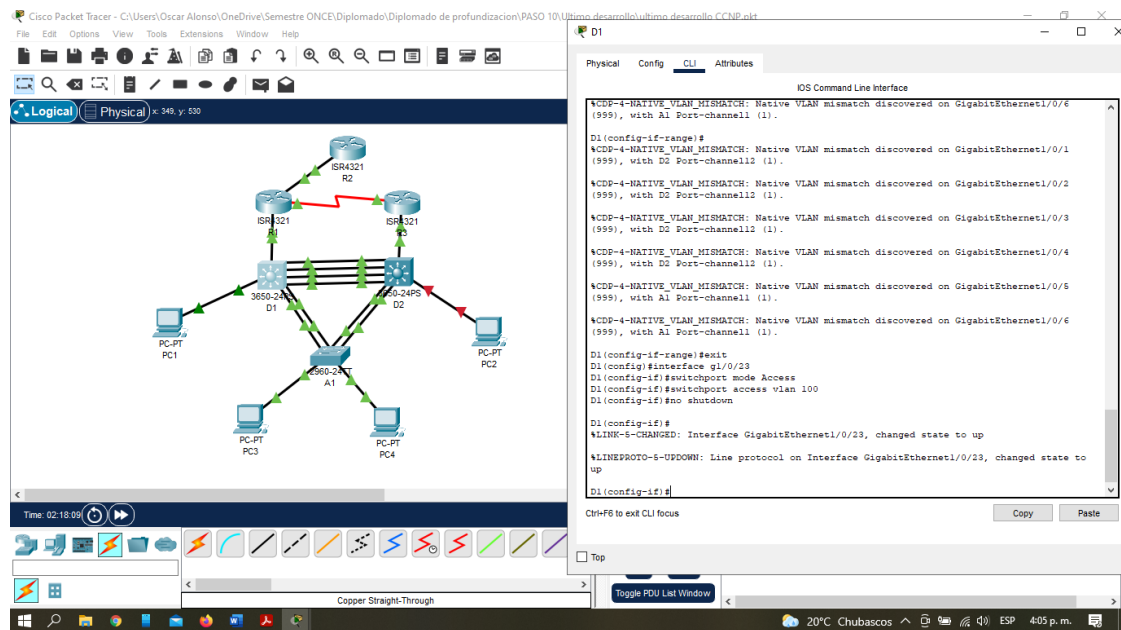


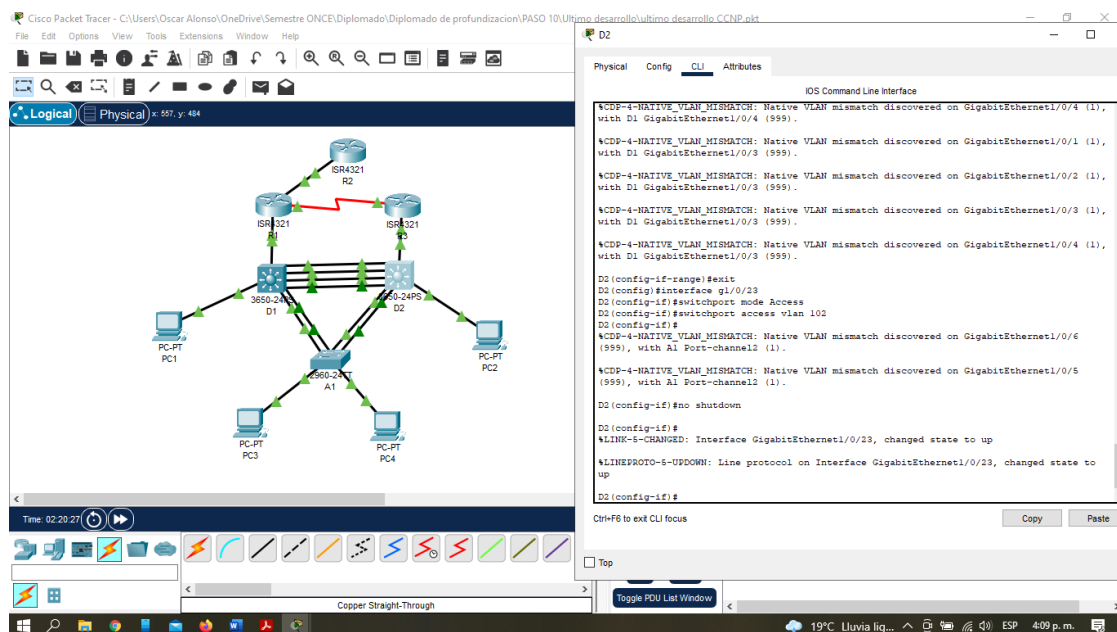
Ilustración 28 configuración puertos de acceso del host D1

Configuración Switch D2

```

D2#configure terminal
D2(config)#interface g1/0/23
D2(config-if)#switchport mode Access
D2(config-if)#switchport access vlan 102
D2(config-if)#no shutdown

```



Configuración Switch A1

```

A1#configure terminal
A1(config)#interface f0/23
A1(config-if)#switchport mode Access
A1(config-if)#switchport access vlan 101
A1(config-if)#no shutdown
A1(config-if)#interface f0/24
A1(config-if)#switchport mode Access
A1(config-if)#switchport access vlan 100
A1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed
state to up
A1(config-if)#no shutdown
A1(config-if)#

```

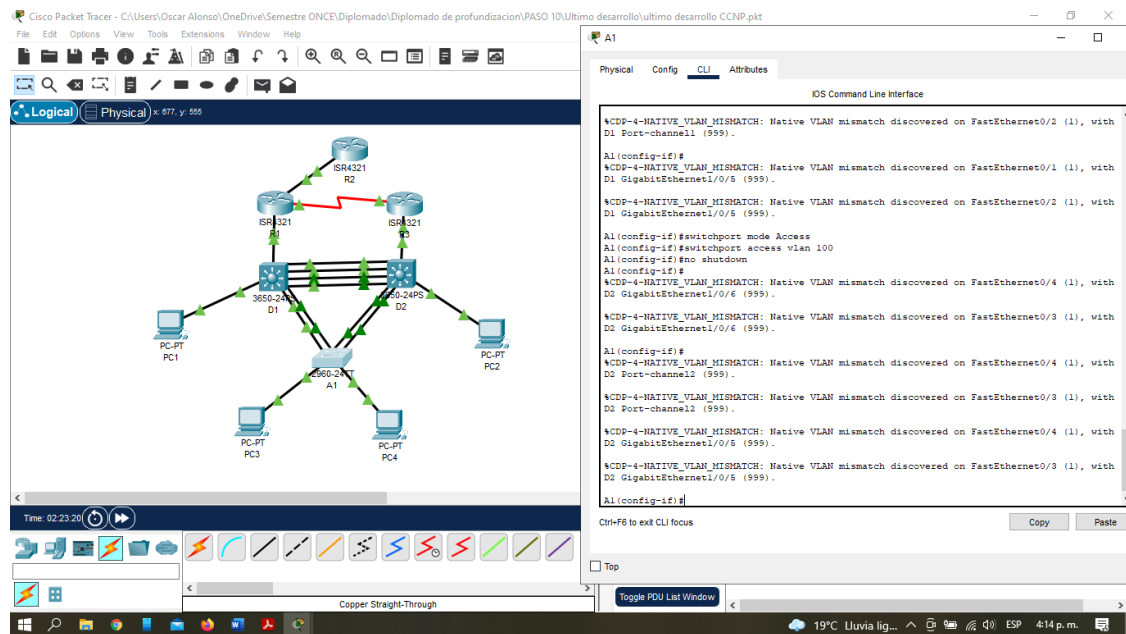


Ilustración 30 configuración puertos de acceso del host A1

2.7 Verifique los servicios DHCP IPv4.

Configuración DHCP IPv4 en PC2

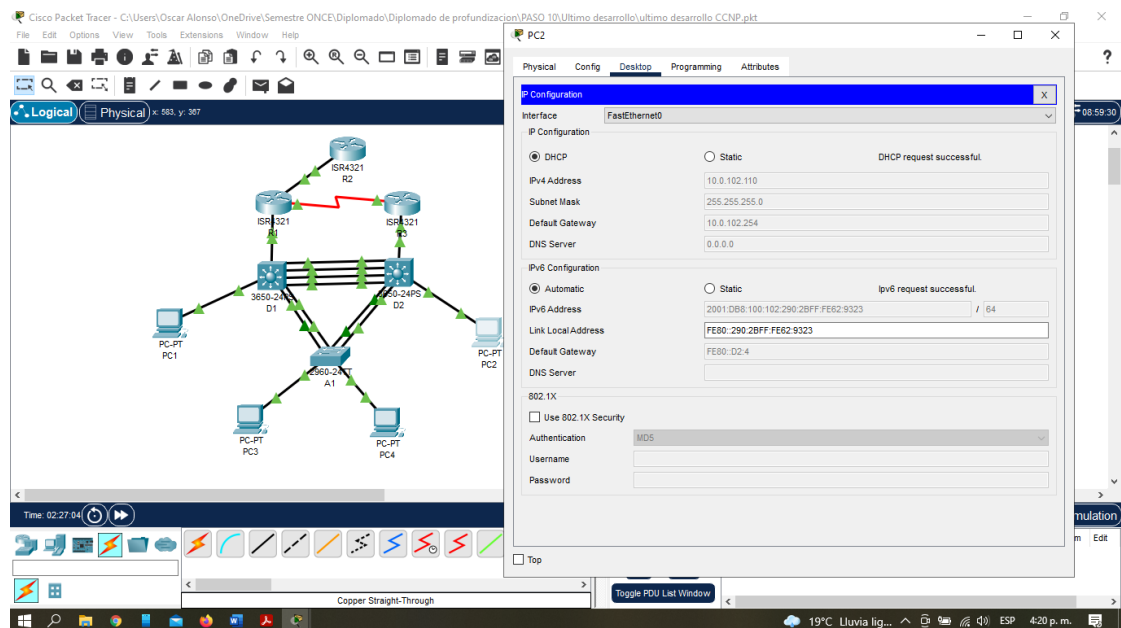


Ilustración 31 DHCP IPv4 en PC2

Configuración DHCP IPv4 en PC2

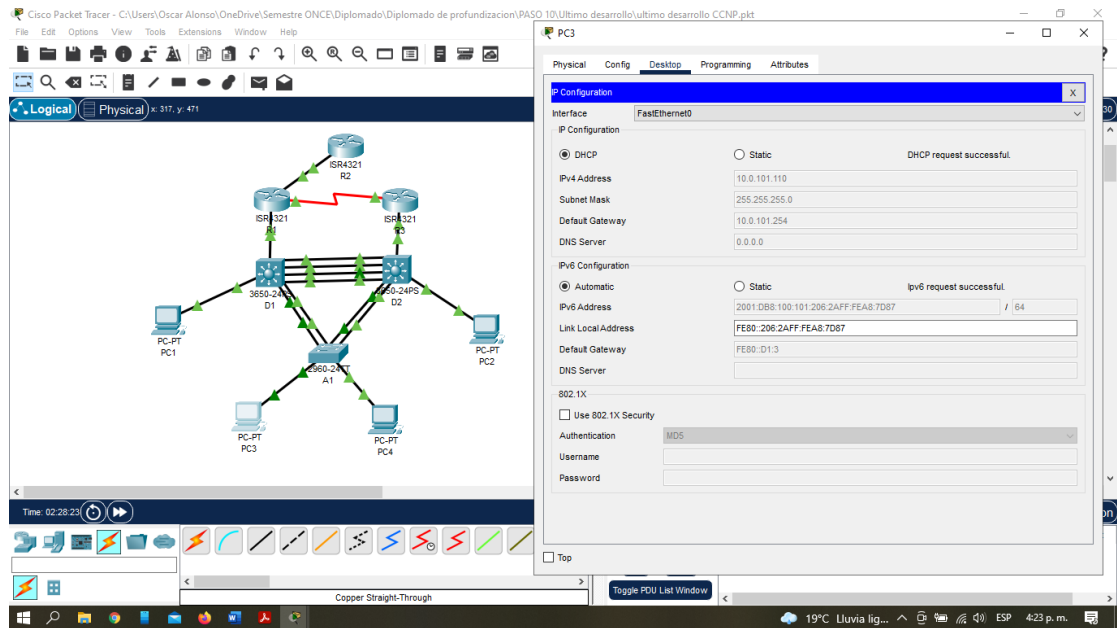


Ilustración 32 DHCP IPv4 en PC3

2.8 Verifique la conectividad de la LAN local

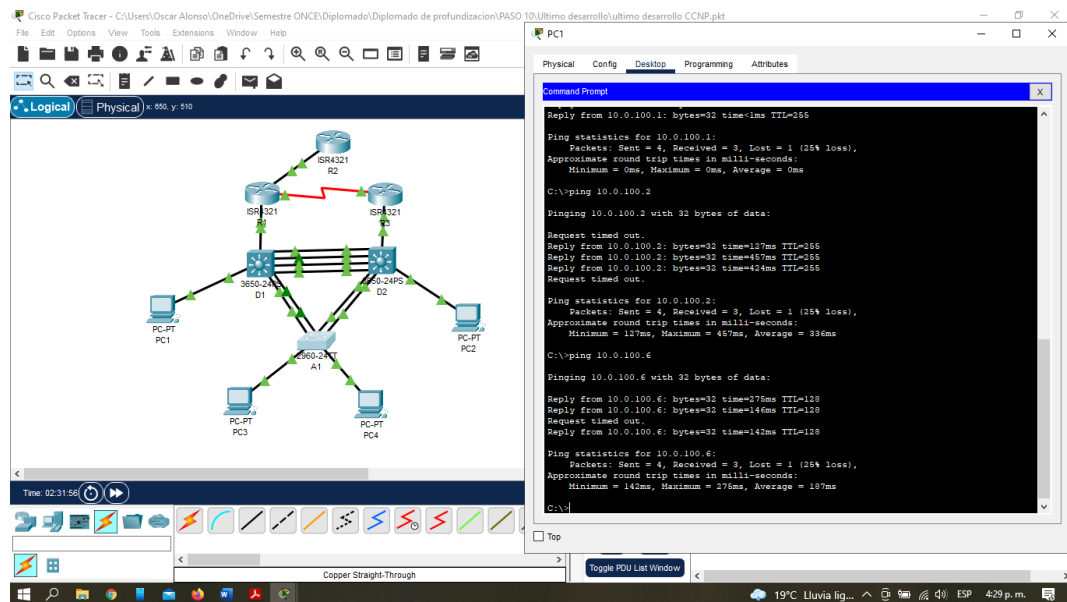


Ilustración 33 Condiciones de conectividad PC1

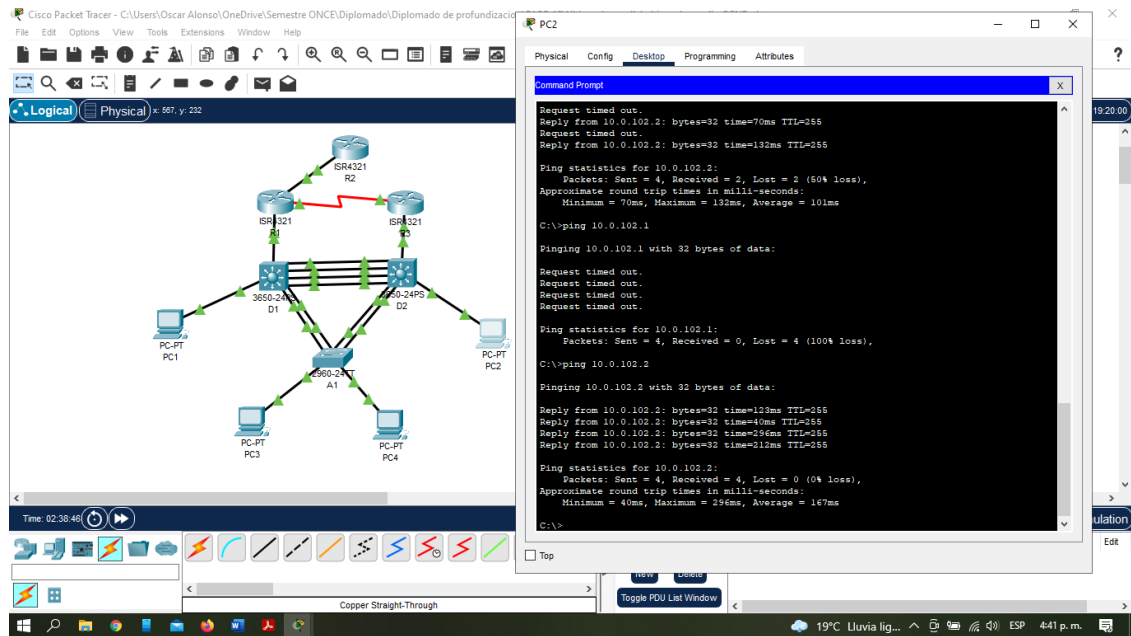


Ilustración 34 Condiciones de conectividad PC2

3 Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Las tareas de configuración son las siguientes:

Tabla 3 Configurar los protocolos de enrutamiento

Tarea#	Tarea	Especificación
--------	-------	----------------

3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.	<p>Use OSPF Process ID 4 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	<p>Use OSPF Process ID 6 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.3	En R2 en la “Red ISP”, configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). <p>La ruta por defecto (::/0).</p>

3.4	<p>En R1 en la “Red ISP”, configure MP-BGP.</p>	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. <p>En IPv6 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. <p>Anuncie la red 2001:db8:100::/48.</p>
-----	---	--

3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.

Configuración Router R1

```

R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#

```

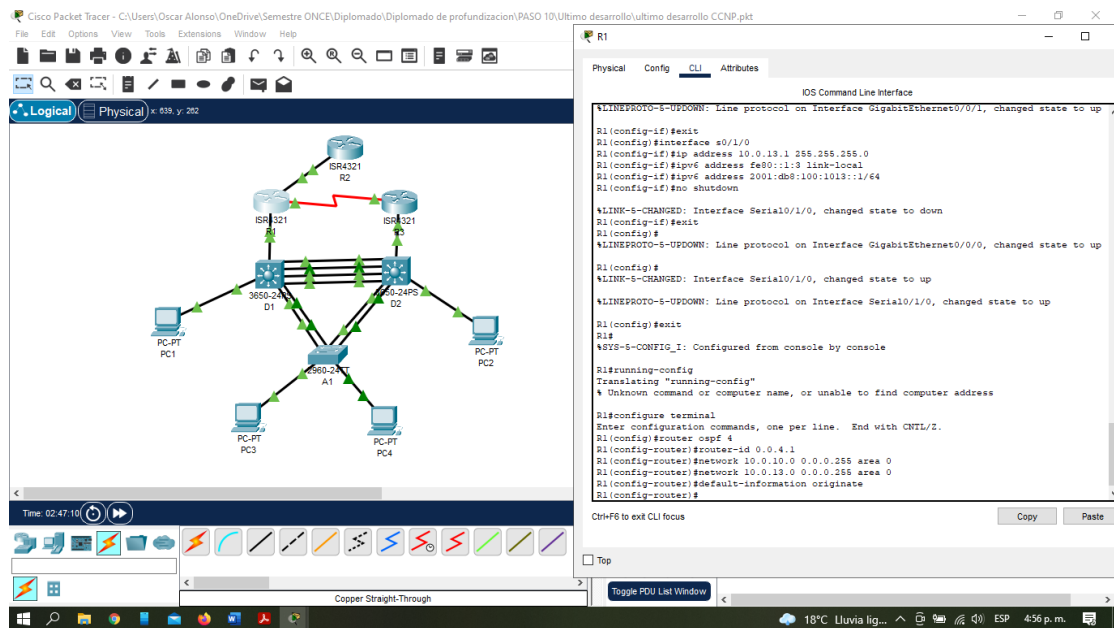



Ilustración 35 configuración single-area OSPFv2 en area 0 en R1

Configuración Router R3

```

R3#configure terminal
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
R3(config-router)#
00:34:29: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial0/1/0
from LOADING to FULL, Loading Done

```

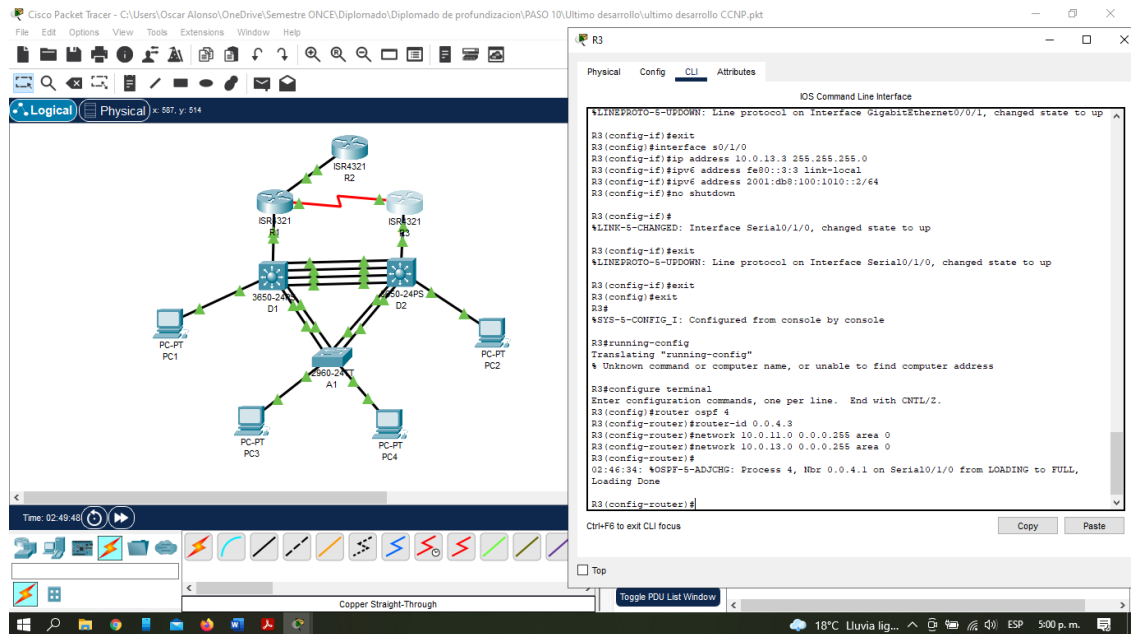


Ilustración 36 configuración single-area OSPFv2 en area 0 en R3

Configuración Switch D1

```

D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#passive-interface g1/0/1
D1(config-router)#passive-interface g1/0/2
D1(config-router)#passive-interface g1/0/3
D1(config-router)#passive-interface g1/0/4
D1(config-router)#passive-interface g1/0/5
D1(config-router)#passive-interface g1/0/6
D1(config-router)#passive-interface g1/0/7
D1(config-router)#passive-interface g1/0/8
D1(config-router)#passive-interface g1/0/9
D1(config-router)#passive-interface g1/0/10
D1(config-router)#passive-interface g1/0/12
D1(config-router)#passive-interface g1/0/13
D1(config-router)#passive-interface g1/0/14
D1(config-router)#passive-interface g1/0/15
D1(config-router)#passive-interface g1/0/16
D1(config-router)#passive-interface g1/0/17
  
```

```

D1 (config-router)#passive-interface g1/0/18
D1 (config-router)#passive-interface g1/0/19
D1 (config-router)#passive-interface g1/0/20
D1 (config-router)#passive-interface g1/0/21
D1 (config-router)#passive-interface g1/0/22
D1 (config-router)#passive-interface g1/0/23
D1 (config-router)#passive-interface g1/0/24
D1 (config-router)#passive-interface g1/1/1
D1 (config-router)#passive-interface g1/1/2
D1 (config-router)#passive-interface g1/1/3
D1 (config-router)#passive-interface g1/1/4

```

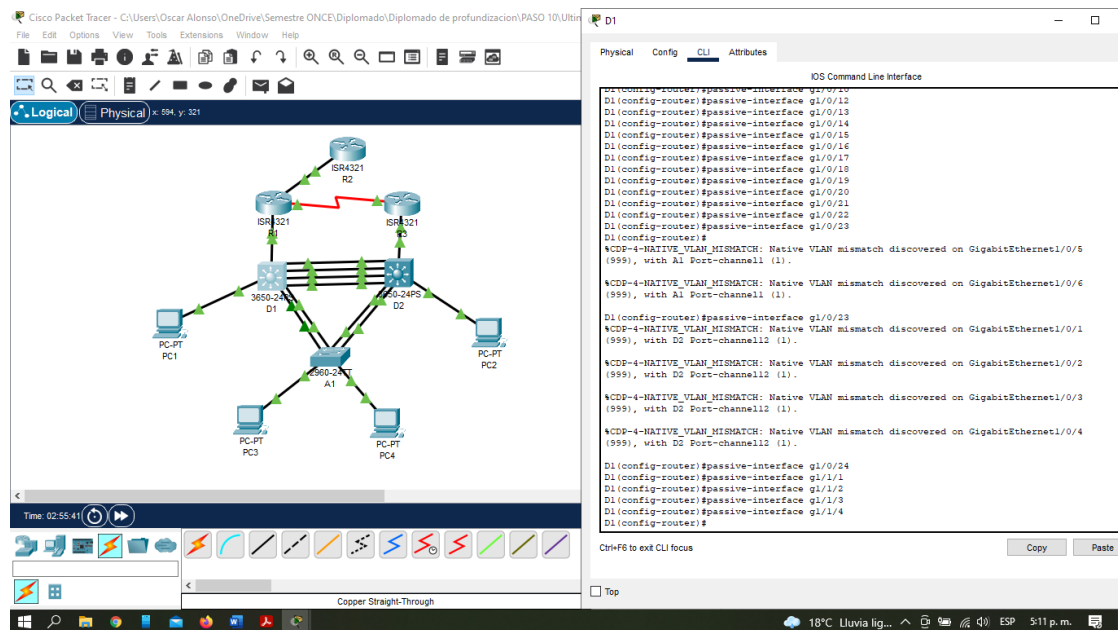


Ilustración 37 configuración single-area OSPFv2 en area 0 en D1

Configuración Switch D2

```

D2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2 (config)#router ospf
D2 (config-router)#router-id 0.0.4.132
D2 (config-router)#network 10.0.11.0 0.0.0.255 area 0
D2 (config-router)#network 10.0.100.0 0.0.0.255 area 0
D2 (config-router)#network 10.0.101.0 0.0.0.255 area 0
D2 (config-router)#network 10.0.102.0 0.0.0.255 area 0
D2 (config-router)#passive-interface g1/0/1
D2 (config-router)#passive-interface g1/0/2
D2 (config-router)#passive-interface g1/0/3
D2 (config-router)#passive-interface g1/0/4
D2 (config-router)#passive-interface g1/0/5
D2 (config-router)#passive-interface g1/0/6

```

```

D2 (config-router)#passive-interface g1/0/7
D2 (config-router)#passive-interface g1/0/8
D2 (config-router)#passive-interface g1/0/9
D2 (config-router)#passive-interface g1/0/10
D2 (config-router)#passive-interface g1/0/12
D2 (config-router)#passive-interface g1/0/13
D2 (config-router)#passive-interface g1/0/14
D2 (config-router)#passive-interface g1/0/15
D2 (config-router)#passive-interface g1/0/16
D2 (config-router)#passive-interface g1/0/17
D2 (config-router)#passive-interface g1/0/18
D2 (config-router)#passive-interface g1/0/19
D2 (config-router)#passive-interface g1/0/20
D2 (config-router)#passive-interface g1/0/21
D2 (config-router)#passive-interface g1/0/22
D2 (config-router)#passive-interface g1/0/23
D2 (config-router)#passive-interface g1/0/24
D2 (config-router)#passive-interface g1/1/1
D2 (config-router)#passive-interface g1/1/2
D2 (config-router)#passive-interface g1/1/3 ospf
D2 (config-router)#passive-interface g1/1/4

```

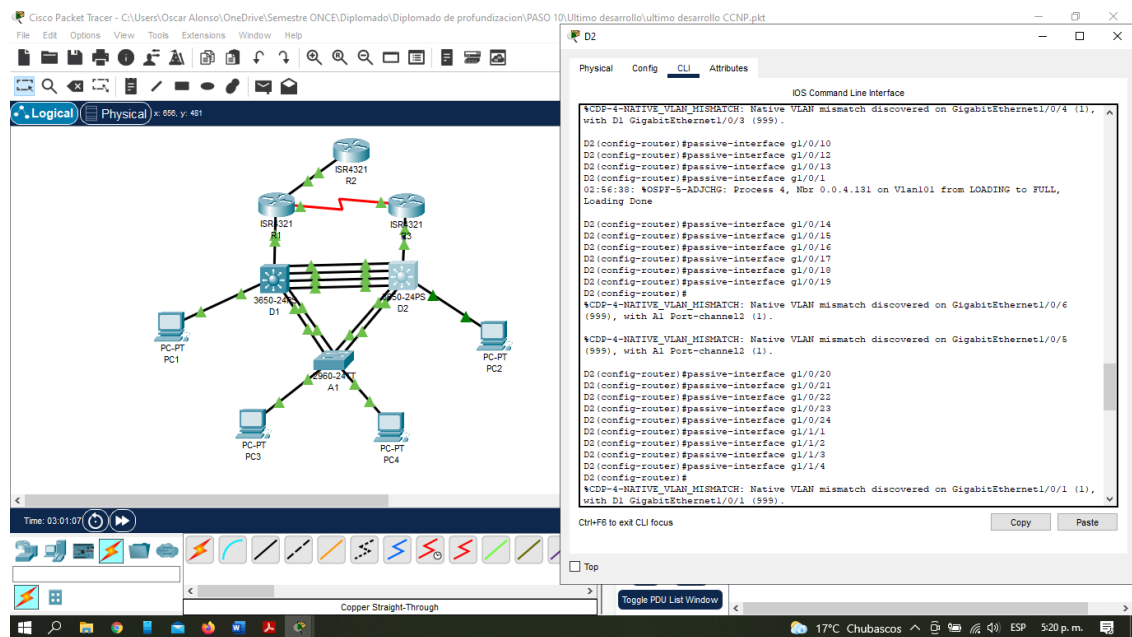


Ilustración 38 configuración single-area OSPFv2 en area 0 en D2

3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.

Configuración Router R1

```

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#interface g0/0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#interface s0/1/0
R1(config-if)#ipv6 ospf 6 area 0

```

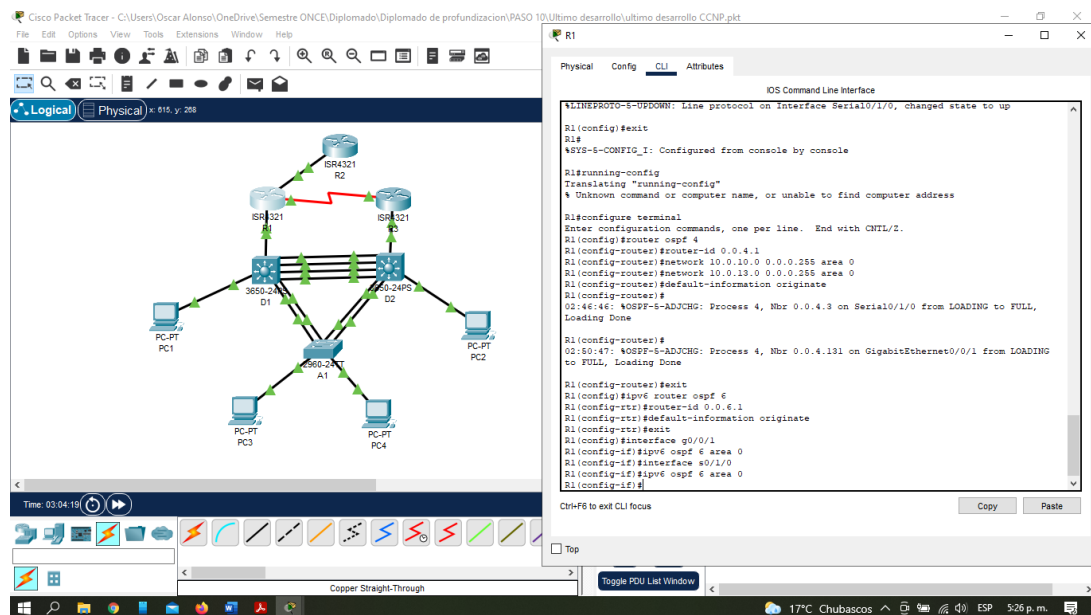


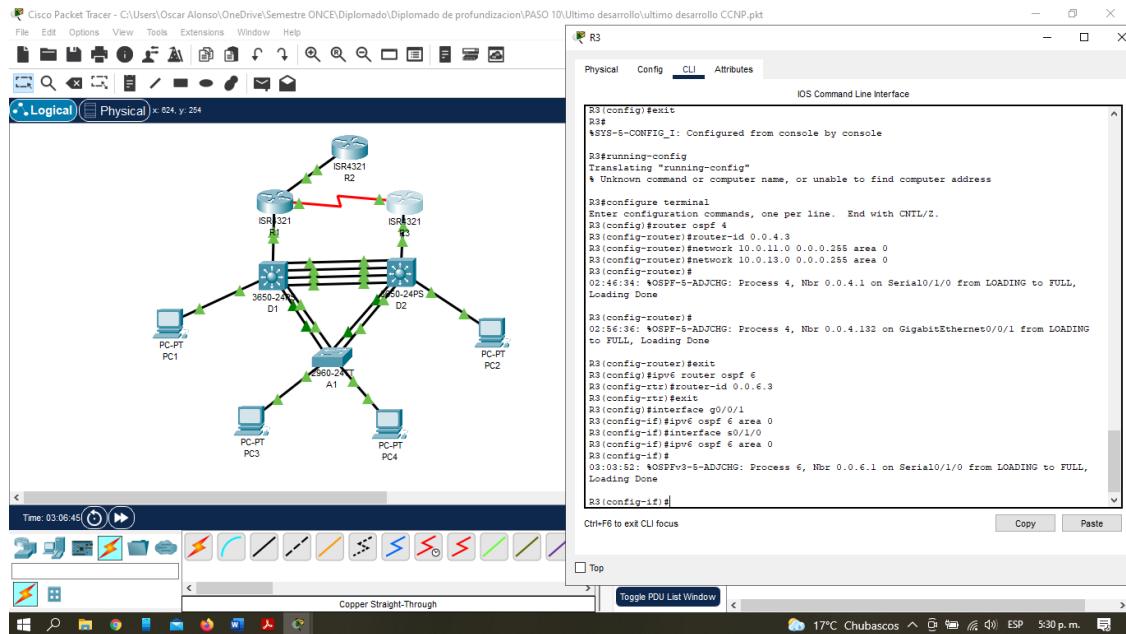
Ilustración 39 configuración classic single-area OSPFv3 en area 0 en R1

Configuración Router R3

```

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface g0/0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#interface s0/1/0
R3(config-if)#ipv6 ospf 6 area 0

```



Configuración Swich D1

```
D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#exit
D1(config)#interface g1/0/11
D1(config-if)#ipv6 ospf 6 area 0
D1(config)#inter vlan100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#inter vlan101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#inter vlan102
D1(config-if)#ipv6 ospf 6 area 0
```

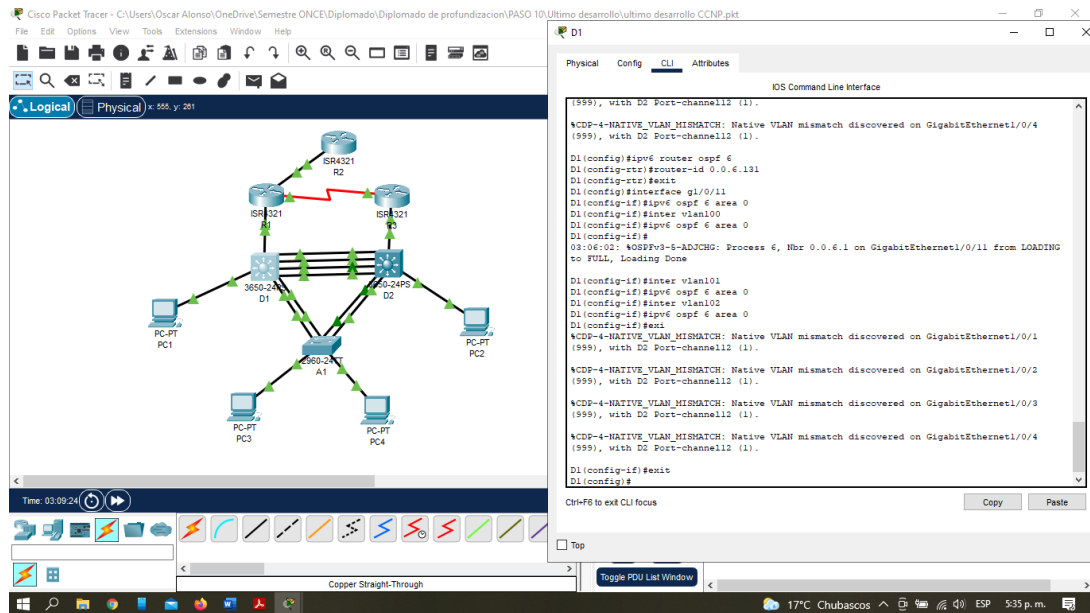


Ilustración 41 configuración classic single-area OSPFv3 en area 0 en D1

Configuración Switch D2

D2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#ipv6 router ospf 6

D2(config-rtr)#router-id 0.0.6.132

D2(config-rtr)#

D2(config-rtr)#exit

D2(config)#interface g1/0/11

D2(config-if)#ipv6 router ospf 6 area 0

D2(config-if)#ipv6 ospf 6 area 0

D2(config-if)#interface vln100

D2(config-if)#ipv6 ospf 6 area 0

D2(config-if)#interface vln101

D2(config-if)#ipv6 ospf 6 area 0

D2(config-if)#interface vln102

D2(config-if)#ipv6 ospf 6 area 0

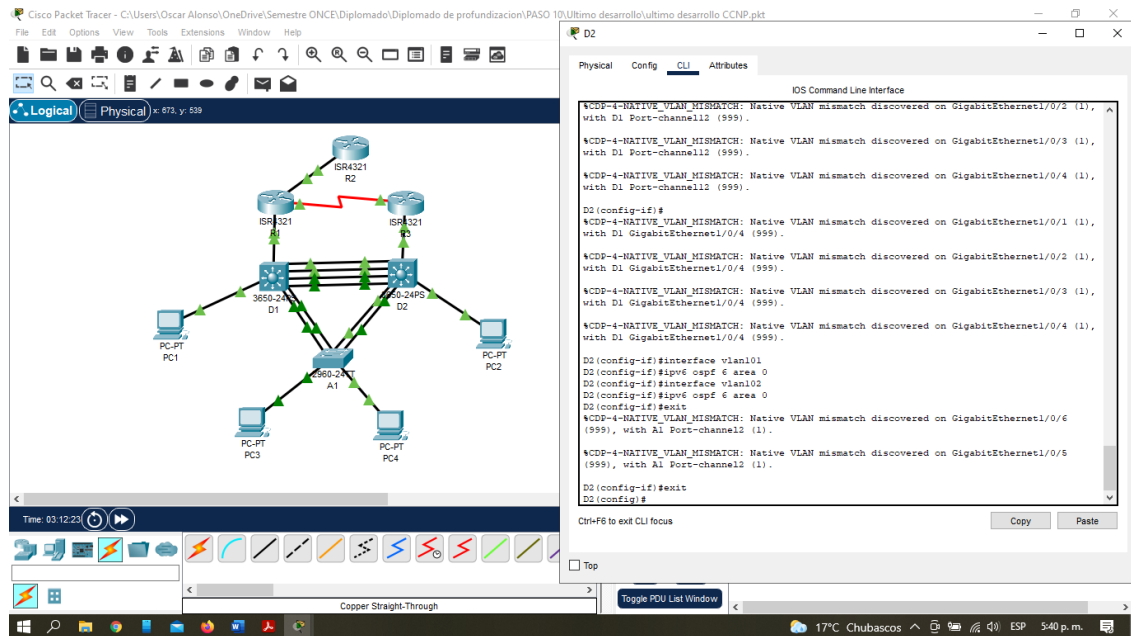


Ilustración 42 configuración classic single-area OSPFv3 en area 0 en D2

3.3 En R2 en la “Red ISP”, configure MP-BGP.

Configuración Router R2

```

R2>enable
R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R2(config)#ipv6 route ::/0 loopback 0 predetermined
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300
R2(config-router)# address-family ipv4 unicast
R2(config-router)#network 2.2.2.2 mask 255.255.255.255
R2(config-router)#network 0.0.0.0 mask 0.0.0.0
R2(config-router)# address-family ipv6 unicast
R2(config-router-af)# network 2001:db8:200::1 /128
R2(config-router-af)# network ::/0
  
```

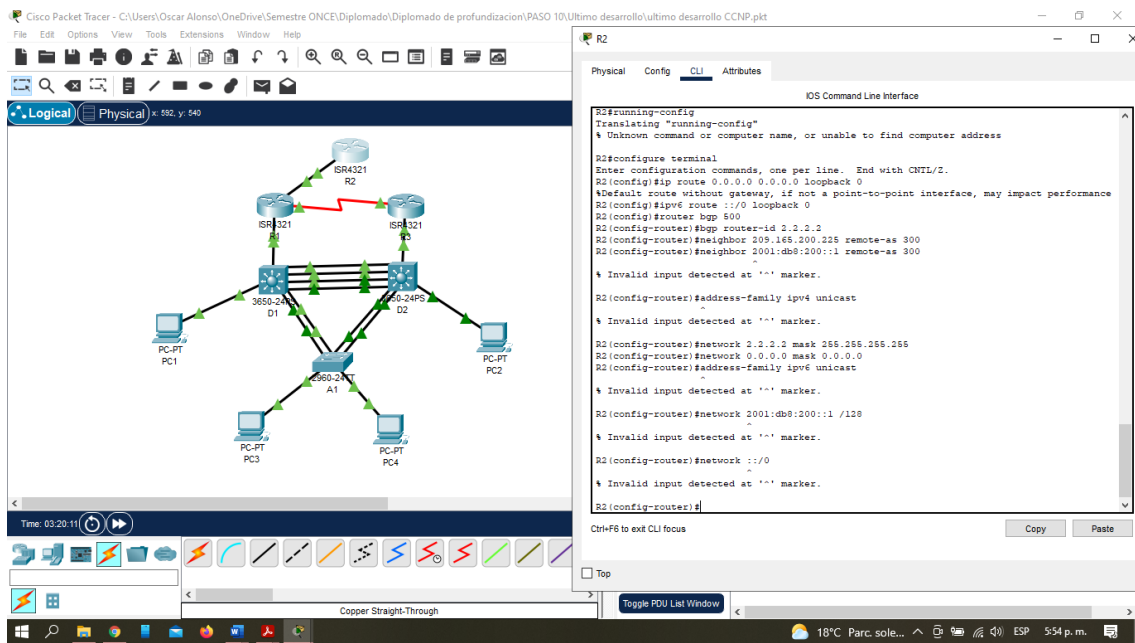



Ilustración 43 configuración MP-BGP en R2

3.4 En R1 en la “Red ISP”, configure MP-BGP.

Configuración Router R2

```

R1>enable
R1#configure terminal
R1(config)#ip route 10.0.0.0 255.255.255.0 null 0
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R2(config-router)# address-family ipv4 unicast
R1(config-router)# address-family ipv6 unicast
R1(config-router-af)# network 2001:db8:200::1 /128
  
```

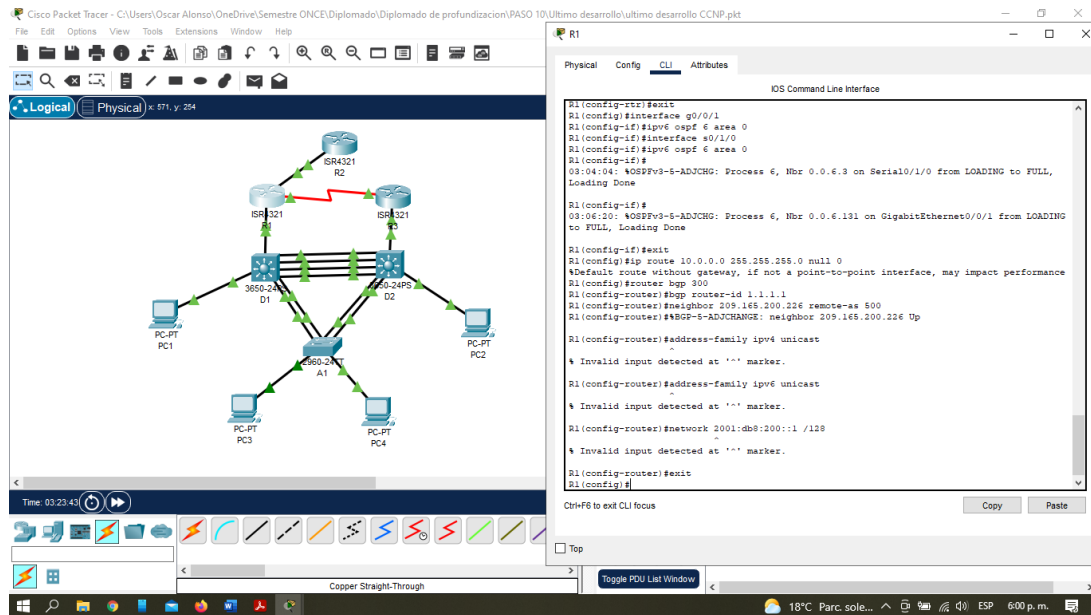


Ilustración 44 configuración MP-BGP en R1

4 Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

En esta parte, debe configurar HSRP version 2 para proveer redundancia de primer salto para los host en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

Tabla 4 Configurar la Redundancia del Primer Salto (First Hop Redundancy)

Tarea#	Tarea	Especificación
--------	-------	----------------

4.1	<p>En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.</p>	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R1G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sintiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	<p>En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.</p>	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R3G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sintiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and one for IPSLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>

4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). <p>Rastree el objeto 6 y decremente en 60.</p>
-----	-------------------------	--

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

Configuración Switch D1

```
D1#configure terminal
D1(config)#ip sla 4
D1(config-ip-sla)#icmp echo 10.0.10.1 source-interface e2/1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 start-time now life forever
D1(config)#track 4 ip sla 4 state
D1(config-track)#delay up 10 down 15
D1(config-track)#exit
D1(config)#ip sla 6
D1(config-ip-sla)#icmp echo 2001:db8:100:1010::1 source-interface
e2/1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 6 start-time now life forever
D1(config)#track 6 ip sla 6 state
D1(config-track)#delay up 10 down 15
D1(config-track)#exit
```

Nota: el comando SLA no es soportado en la configuración del simulador

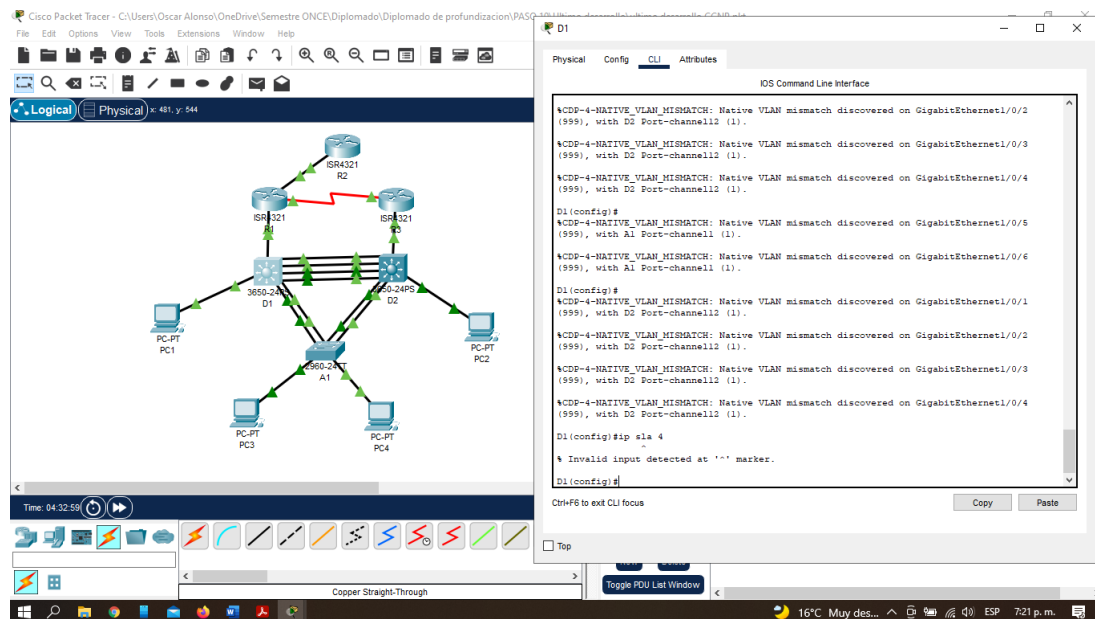


Ilustración 45 accesibilidad de la interfaz R1 G0/0/1

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

Configuración Switch D2

```

D2#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1 source-interface e2/1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 start-time now life forever
D2(config)#track 4 ip sla 4 state
D2(config-track)#delay up 10 down 15
D2(config-track)#exit
D2(config)#
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-interface
e2/1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 6 start-time now life forever
D2(config)#track 6 ip sla 6 state
D2(config-track)#delay up 10 down 15
D2(config-track)#exit
D2(config)#

```

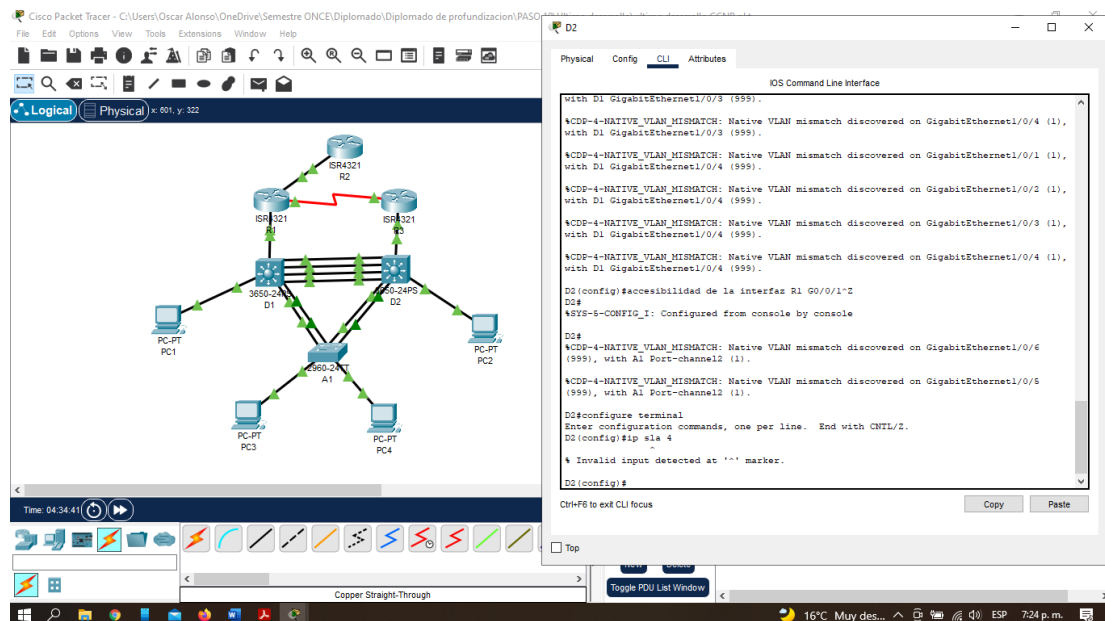


Ilustración 46 cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1

4.3 En D1, configure HSRPv2.

Configuración Switch D1

Grupo 104 vlan 100

```
D1#configure terminal
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 track 4 decrement 60
D1(config-if)#end
```

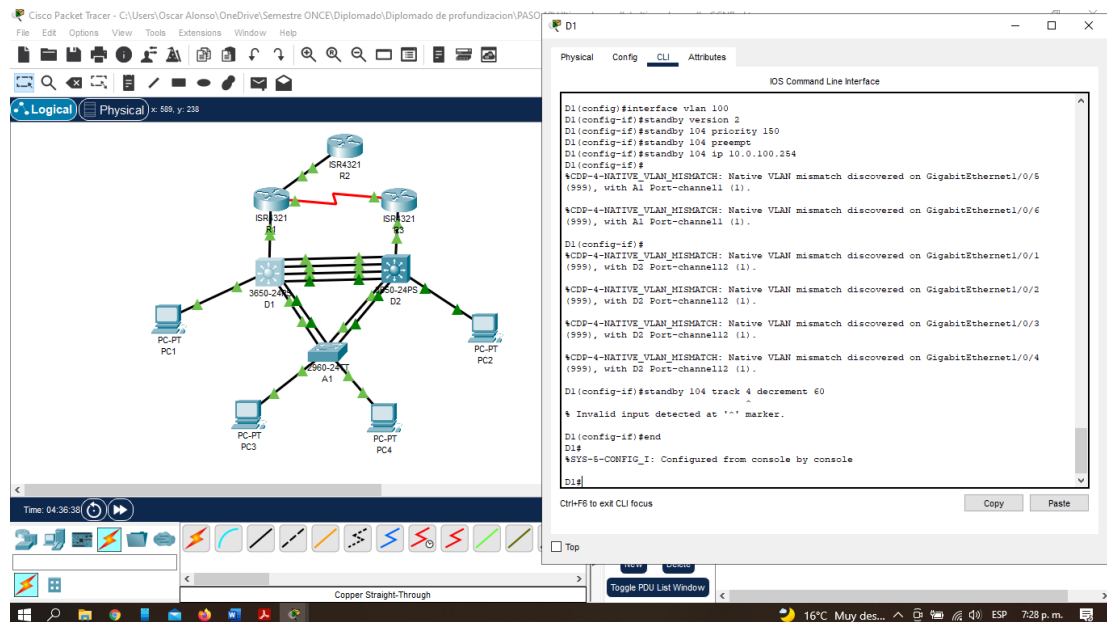


Ilustración 47 Grupo 104 vlan 100

Grupo 114 Vlan 101.

```
D1#configure terminal
D1(config)#interface vlan 101
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby version 2
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#end
```

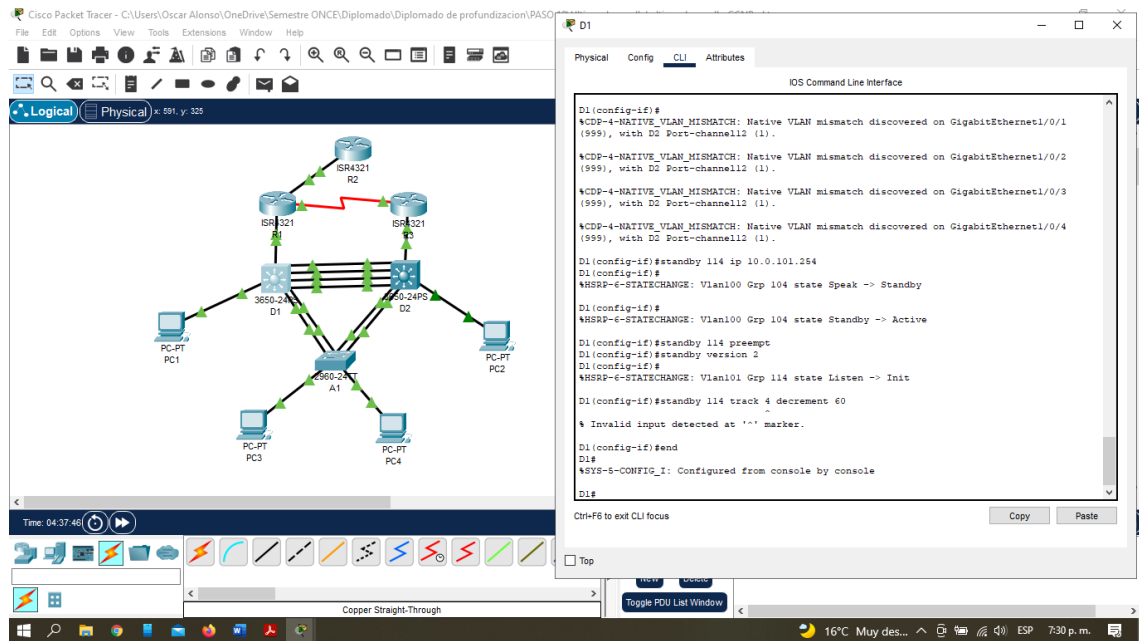


Ilustración 48 Grupo 114 Vlan 101

Grupo 124 vlan 102.

```

D1#configure terminal
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#standby 124 ip 10.0.102.254
D1(config-if)#end
  
```

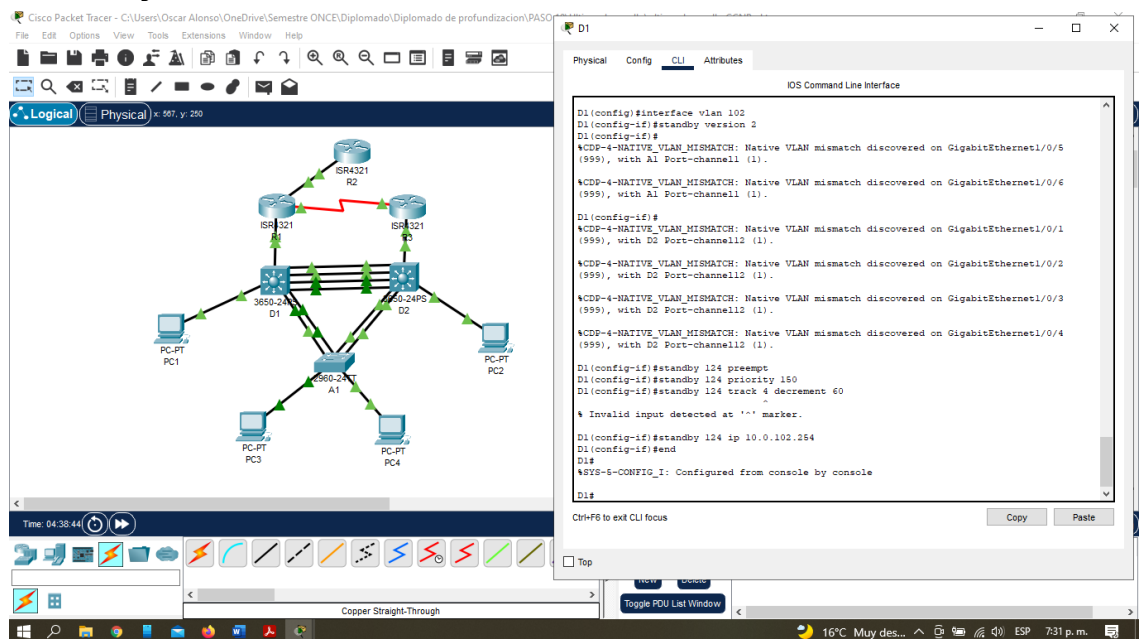


Ilustración 49 Grupo 124 vlan 102.

Grupo 106 vlan 100

```
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#standby ipv6 autoconfig
D1(config-if)#end
```

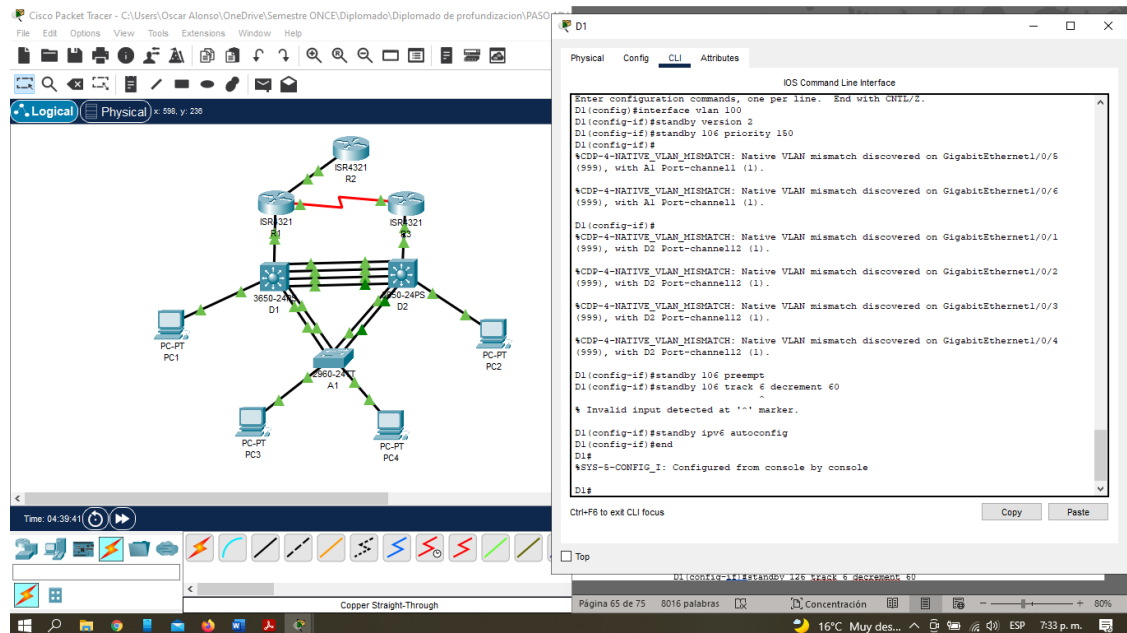
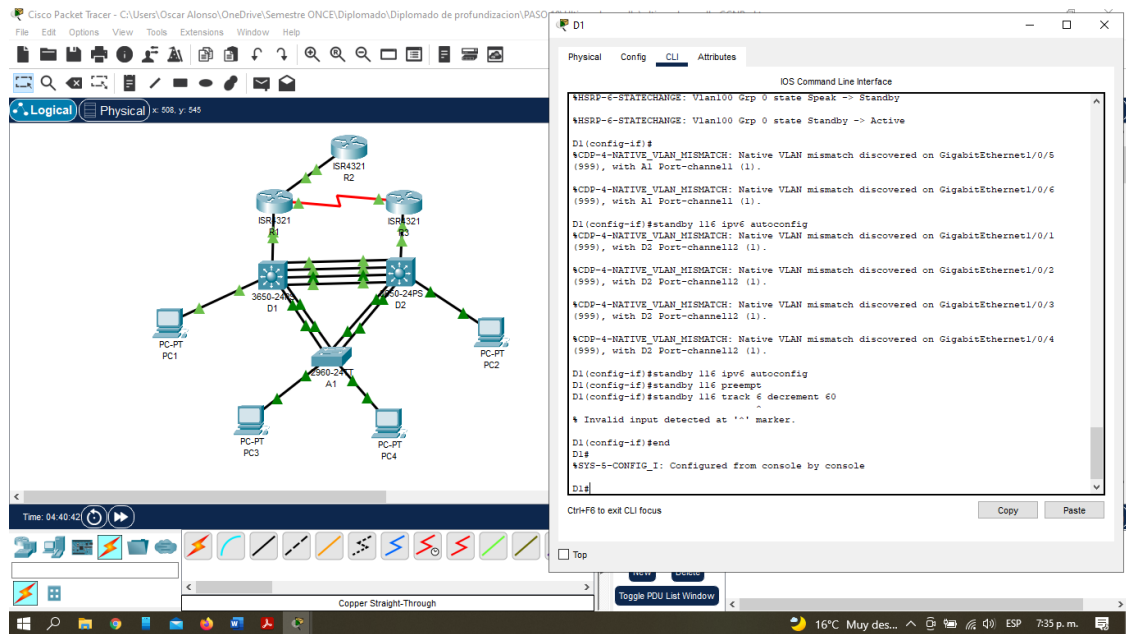


Ilustración 50 Grupo 106 vlan 100

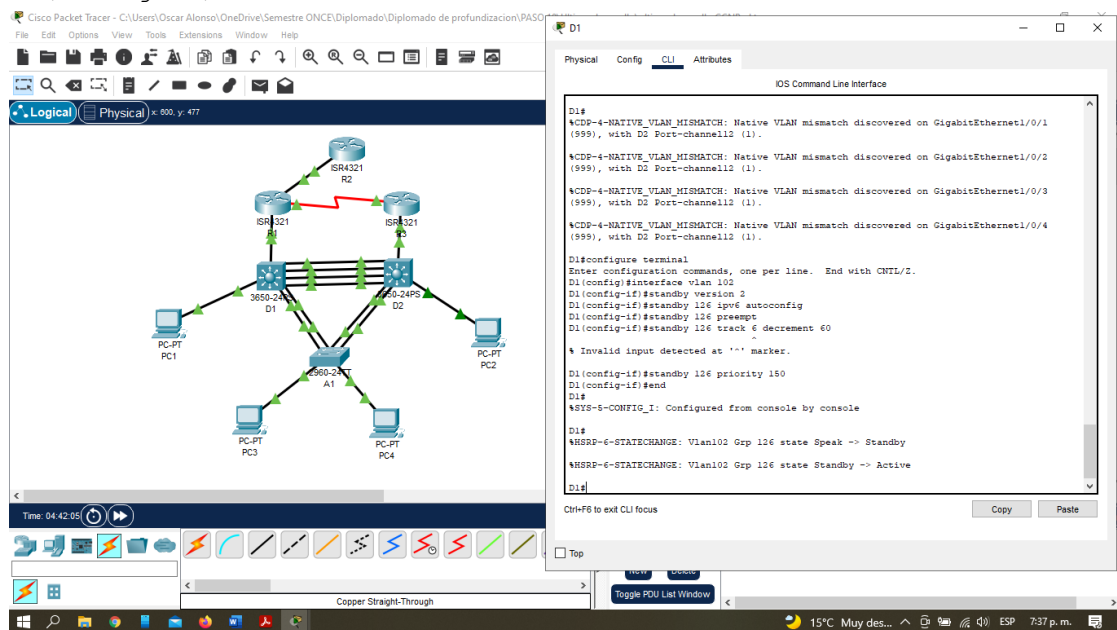
Grupo 116 Vlan 101.

```
D1#configure terminal
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#end
```



Grupo 126 vlan 102

```
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 preempt
D1(config-if)#standby 126 track 6 decrement 60
D1(config-if)#standby 126 priority 150
D1(config-if)#end
```



Configuración Swich D2

Grupo 104 vlan 100

```
D2#configure terminal
D2(config)#interface vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt
D2(config-if)#standby 104 track 4 decrement 60
D2(config-if)#end
```

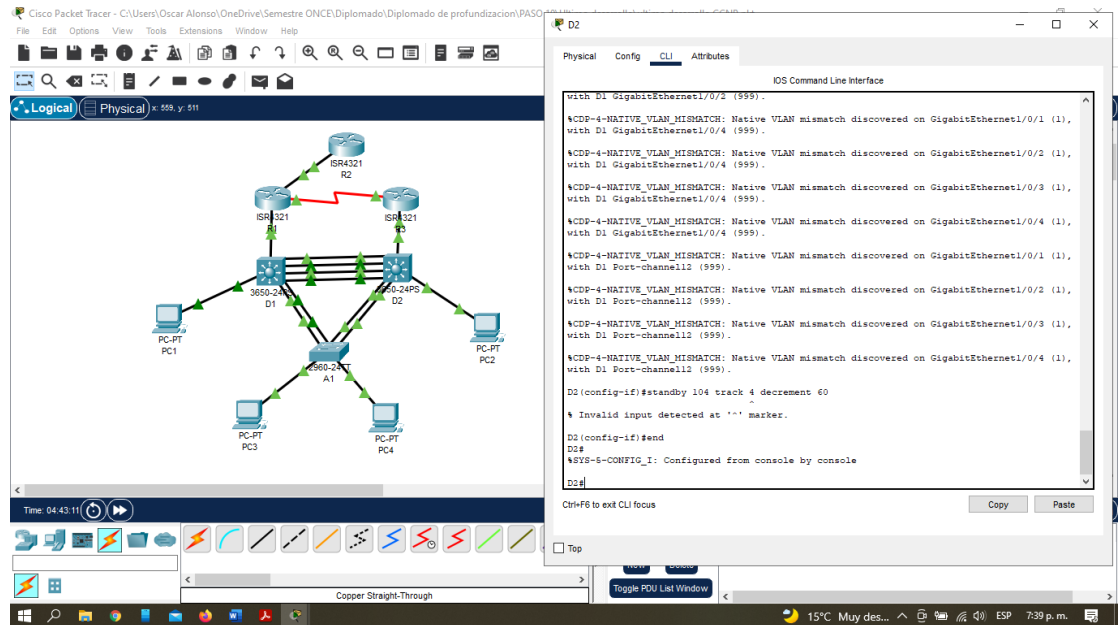


Ilustración 53 Grupo 104 vlan 100

Grupo 114 Vlan 101.

```
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#standby 114 track 4 decrement 60
```

Grupo 124 vlan 102.

```
D2#configure terminal
D2(config)#interface vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
D2(config-if)#standby 124 preempt
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#end
```

Grupo 106 vlan 100

```
D2#configure terminal
D2(config)#interface vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt
D2(config-if)#standby 106 track 6 decrement 60
D2(config-if)#end
```

Grupo 116 Vlan 101.

```
D2#configure terminal
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#end
```

Grupo 126 vlan 102

```
D2#configure terminal
D2(config)#interface vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#standby 126 preempt
D2(config-if)#end
```

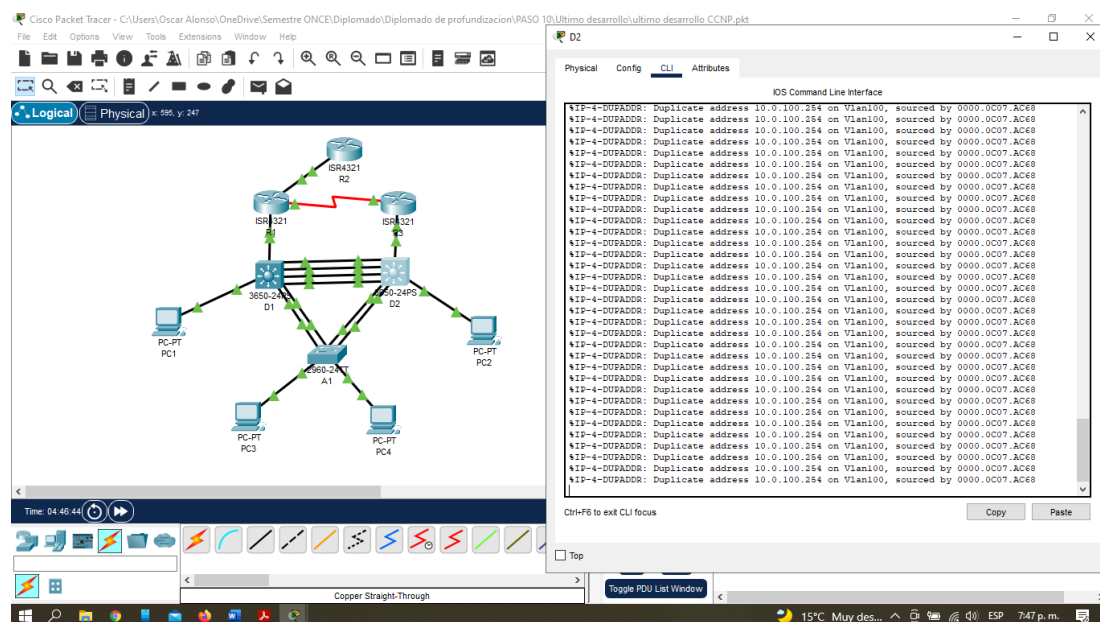


Ilustración 54 Grupo 126 vlan 102

5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de inscripción SCRYPT.

Configuración Router R1

```
R1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

Configuración Router R2

```
R2(config)#enable algorithm-type scrypt secret cisco12345cisco
```

Configuración Router R3

```
R3(config)#enable algorithm-type scrypt secret cisco12345cisco
```

Configuración Switch D1

```
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

Configuración Switch D2

```
D2(config)#enable algorithm-type scrypt secret cisco12345cisco
```

Configuración Switch A1

```
A1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

Nota: El comando no es soportado

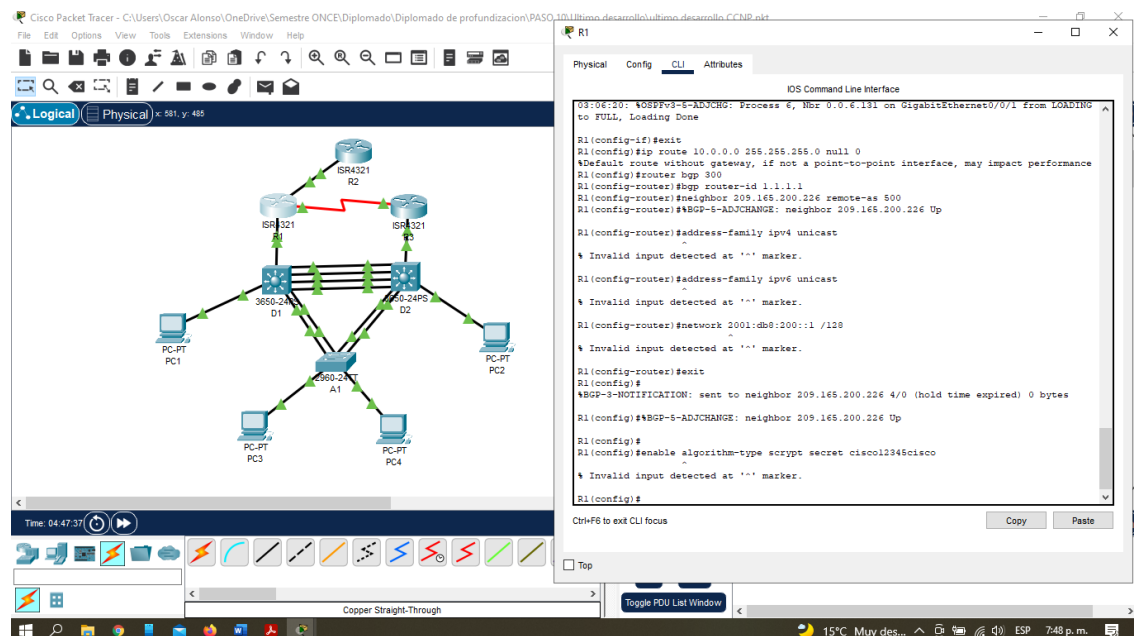


Ilustración 55 protege el EXEC privilegiado usando el algoritmo de inscripción SCRYPT

5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de inscripción SCRYPT.

Configuración Router R1

```
R1(config)#username sadmin privilege 15 secret cisco12345cisco
```

```
R1(config)#
*Nov 12 02:44:07.891: End-
>Password:PxFnRQHeDp9u3TLc8.Sw7QZ8GORUJ3TKPHA71beGWQs
R1(config)#
R1(config)#username sadmin privilege 15 algorithm-type scrypt secret
cisco12345cisco
```

Configuración Router R2

```
R2(config)#username sadmin privilege 15 secret cisco12345cisco
R2(config)#
*Nov 12 02:45:23.645: End-
>Password:PxFnRQHeDp9u3TLc8.Sw7QZ8GORUJ3TKPHA71beGWQs
```

Configuración Router R3

```
R3(config)#username sadmin privilege 15 secret cisco12345cisco
R3(config)#
*Nov 12 02:47:50.572: End-
>Password:PxFnRQHeDp9u3TLc8.Sw7QZ8GORUJ3TKPHA71beGWQs
```

Configuración Switch D1

```
D1(config)#username sadmin privilege 15 secret cisco12345cisco
D1(config)#
```

Configuración Switch D2

```
D2(config)#username sadmin privilege 15 secret cisco12345cisco
```

Configuración Switch A1

```
A1(config)#username sadmin privilege 15 secret cisco12345cisco
```

5.3 En todos los dispositivos (Excepto R2) habilite AAA

Configuración Router R1

```
R1#configure terminal
R1(config)#aaa new-model
```

Configuración Router R3

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#AAA new-model
R3(config)#
```

Configuración Switch D1

```
D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#AAA new-model
D1(config)#
```

Configuración Switch D2

```
D2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#AAA new-model
```

Configuración Switch A1

```
A1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#AAA new-model
```

5.4 En todos los dispositivos (excepto R2) configure las especificaciones del servidor RADIUS.

Configuración Router R1

```
R1#configure terminal
R1(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port
1813 key $strongPass
```

Configuración Router R3

```
R3#configure terminal
R3(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port
1813 key $strongPass
```

Configuración Switch D1

```
D1#configure terminal
D1(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port
1813 key $strongPass
```

Configuración Switch D2

```
D2#configure terminal
D2(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port
1813 key $strongPass
```

Configuración Switch A1

```
A1#configure terminal
```

```
A1(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port  
1813 key $strongPass
```

5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA.

Configuración Router R1

```
R1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#AAA authentication login default group radius local
```

Configuración Router R3

```
R3#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R3(config)#AAA authentication login default group radius local
```

Configuración Switch D1

```
D1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
D1(config)#AAA authentication login default group radius local
```

Configuración Switch D2

```
D2#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
D2(config)#AAA authentication login default group radius local
```

Configuración Switch A1

```
A1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
A1(config)#AAA authentication login default group radius local
```

5.6 Verifique el servicio AAA en todos los dispositivos (except R2).

6 Configure las funciones de Administración de Red.

6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual.

Configuración Router R1

```
R1#clock set 15:27:00 16 oct 2021
```



```
*Nov 16 20:29:57.168: %SYS-6-CLOCKUPDATE: System clock has been
updated from 20:29:57 UTC Tue Nov 16 2021 to 20:29:57 UTC Tue Nov
16 2021, configured from console by sadmin on console.
```

Configuración Router R2

```
R2#clock set 15:27:00 16 oct 2021
*Nov 16 20:29:57.168: %SYS-6-CLOCKUPDATE: System clock has been
updated from 20:29:57 UTC Tue Nov 16 2021 to 20:29:57 UTC Tue Nov
16 2021, configured from console by sadmin on console.
```

Configuración Router R3

```
R3#clock set 15:27:00 16 oct 2021
R3#
Nov 16 20:27:49.843: %SYS-6-CLOCKUPDATE: System clock has been
updated from 20:27:49 UTC Tue Nov 16 2021 to 20:27:49 UTC Tue Nov
16 2021, configured from console by sadmin on console.
```

Configuración Switch D1

```
D1#clock set 15:51:00 16 oct 2021
D1#
```

Configuración Switch D2

```
D1#clock set 15:51:00 16 oct 2021
D1#
```

Configuración Switch A1

```
D1#clock set 15:51:00 16 oct 2021
D1#
```

6.2 Configure R2 como un NTP maestro

Configuración Router R2

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 3
R2(config)#
```

6.3 Configure NTP en R1, R3, D1, D2, y A1.

R1. Sincroniza con R2

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#ntp server 209.165.200.2
R1(config)#end
```

R3 Sincroniza con R1

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp server 10.0.13.1
R3(config)#end
```

D1. Sincroniza con R1

```
D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ntp server 10.0.10.1
D1(config)#end
```

A1. Sincroniza con R1

```
A1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#ntp server 10.0.10.1
A1(config)#end
```

D2. Sincroniza con R3.

```
D2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ntp server 10.0.11.1
D2(config)#end
```

6.4 Configure Syslog en todos los dispositivos excepto en R2.

Configuración Router R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#logging 10.0.100.5
R1(config)#logging trap warnings
```

Configuración Router R3

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#logging 10.0.100.5
R3(config)#logging trap warnings
```

Configuración Switch D1

```
D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#logging 10.0.100.5
```

```
D1(config)#logging trap warnings
```

Configuración Switch D2

```
D2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#logging 10.0.100.5
D2(config)#logging trap warnings
```

Configuración Switch A1

```
A1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#logging 10.0.100.5
A1(config)#logging trap warnings
```

6.5 Configure SNMPv2c en todos los dispositivos excepto R2.

Configuración Router R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#snmp-server community ENCORSA ro
R1(config)#snmp-server contact Helman Alfonso
R1(config)#snmp-server enable traps bgp
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
```

Configuración Router R3

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#snmp-server community ENCORSA ro
R3(config)#snmp-server contact Helman Alfonso
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
```

Configuración Switch D1

```
D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#snmp-server community ENCORSA ro
D1(config)#snmp-server contact Helman Alfonso
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf
```

Configuración Switch D2

D2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#snmp-server community ENCORSA ro

D2(config)#snmp-server contact Helman Alfonso

D2(config)#snmp-server enable traps config

D2(config)#snmp-server enable traps ospf

Configuración Switch A1

A1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

A1(config)#snmp-server community ENCORSA ro

A1(config)#snmp-server contact Helman Alfonso

A1(config)#snmp-server enable traps config

CONCLUSIONES

El desarrollo de la anterior evaluación de conocimientos nos ha permitido enriquecer los conocimientos adquiridos hasta el momento donde observamos verdaderamente que existen funciones amplias dentro del portafolio de comandos que permiten brindar protección y seguridad a un determinado cliente que requiere servicios de almacenamiento y transferencia de datos.

La seguridad informática debe estar siempre a la vanguardia en el desarrollo de los software y dispositivos tecnológicos de comunicación, para ellos existen comandos que protegen los sistemas informáticos, realizan bloqueos de direcciones no confirmadas dentro de sus tablas, eliminando el riesgo en la pérdida de información.

El desarrollo de una red informática puede abarcar un número amplio de configuraciones, todas y cada una de ellas dependen de los requerimientos de un determinado cliente y la capacidad de inversión a la que se quiera llegar, estas configuraciones van desde redes muy pequeñas que se pueden hallar en una hoja o pequeña oficina, hasta las redes tan amplias que manejan industrias y compañías que atraviesan grandes terrenos como se vio anteriormente incluso fuera del planeta.

La elección de las configuraciones y equipos siempre estarán acorde a los requerimientos del cliente, es importante resaltar que todos y cada uno de ellos desde los más básicos hasta los grandes servidores deben contar con normas mínimas legales de operación, funcionamiento y protección a personas, brindando seguridad en el resguardo de la información que por ellos se mueve.

BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **Foundational Network Programmability Concepts**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **Introduction to Automation Tools**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **Secure Access Control**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **Network Device Access Control and Infrastructure Security**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **Virtualization**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>